*ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ*

*ЧАМЗИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА*

*Является официальным печатным изданием*

*Чамзинского муниципального района*

*11 октября 2019г. № 23 (238)*

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

19 августа 2019 г. № 619

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Реестр молодых семей» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Реестр молодых семей» администрации Чамзинского муниципального района

Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Реестр молодых семей» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Реестр молодых семей» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

3. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия  от «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г. № \_\_ |

**Состав и содержание мер защиты информации (базовый набор)**

**для информационной системы «Реестр молодых семей»**

**Администрации Чамзинского муниципального района**

**Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 3](#_Toc522780427)

[1. Введение 4](#_Toc522780428)

[2. Требования к мерам защиты информации, содержащейся в ИС «Реестр молодых семей» 4](#_Toc522780429)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc522780430)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 5](#_Toc522780431)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc522780432)

[3.3. Ограничение программной среды 6](#_Toc522780433)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc522780434)

[3.5. Регистрация событий безопасности 7](#_Toc522780435)

[3.6. Антивирусная защита 8](#_Toc522780436)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc522780437)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc522780438)

[3.9. Защита среды виртуализации 9](#_Toc522780439)

[3.10. Защита технических средств 9](#_Toc522780440)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc522780441)

[4. Состав и содержание компенсирующих мер 10](#_Toc522780442)

[5. Заключение 16](#_Toc522780443)

Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в информационной системе (далее – ИС) третьего класса защищенности «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в ИС «Реестр молодых семей»

Организационные и технические меры защиты информации, реализуемые в ИС «Реестр молодых семей» Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от 13.08.2019 г. № 234 «Об утверждении документов по защите документов».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| Приложение №2 к постановлению |
| администрации Чамзинского муниципального района  Республики Мордовия |
| от «\_\_\_» \_\_\_\_ 2019 г. № \_\_ |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** информационной системы (далее – ИС) «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ИС «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ИС «Реестр молодых семей».

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ИС «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Приложение №3 к постановлению | | администрации Чамзинского муниципального района  Республики Мордовия | | от «\_\_\_» \_\_\_\_ 2019 г. № \_\_ | |
|  |
|  |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в информационной системе «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в информационной системе (далее – ИС) «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **Информационная система «Реестр молодых семей»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ИС «Реестр молодых семей» Администрации исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства ИС Администрации Чамзинского муниципального района Республики Мордовия располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы д. 1.

Информационное взаимодействие в ИС организовано на базе локальных вычислительных сетей, построенных по стандарту IEEE 802.3u. Рабочие станции имеют подключения к информационно-телекоммуникационным сетям международного информационного обмена. Линии связи не выходят за пределы контролируемой зоны.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемESET NOT 32.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ИС «Реестр молодых семей» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В. Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

19 августа 2019 г. № 620

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Реестр опекаемых детей» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Реестр опекаемых детей» администрации Чамзинского муниципального района

Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе ««Реестр опекаемых детей» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

3. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе ««Реестр опекаемых детей» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского  муниципального района  Республики Мордовия  от «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г. № \_\_ |

**Состав и содержание мер защиты информации (базовый набор)**

**для информационной системы «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 4](#_Toc520298569)

[1. Введение 5](#_Toc520298570)

[2. Требования к мерам защиты информации, содержащейся в ИС «Реестр опекаемых детей» 5](#_Toc520298571)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 6](#_Toc520298572)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 6](#_Toc520298573)

[3.2. Управление доступом субъектов доступа к объектам доступа 7](#_Toc520298574)

[3.3. Ограничение программной среды 7](#_Toc520298575)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 8](#_Toc520298576)

[3.5. Регистрация событий безопасности 8](#_Toc520298577)

[3.6. Антивирусная защита 9](#_Toc520298578)

[3.7. Контроль (анализ) защищенности информации 9](#_Toc520298579)

[3.8. Обеспечение целостности информационной системы и информации 10](#_Toc520298580)

[3.9. Защита среды виртуализации 10](#_Toc520298581)

[3.10. Защита технических средств 10](#_Toc520298582)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 11](#_Toc520298583)

[4. Состав и содержание компенсирующих мер 12](#_Toc520298584)

[5. Заключение 17](#_Toc520298585)

**Обозначения и сокращения**

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в информационной системе третьего класса защищенности «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в ИС «Реестр опекаемых детей»

Организационные и технические меры защиты информации, реализуемые в ИС «Реестр опекаемых детей» Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в информационной системе «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г. № 234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В информационной системе «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| Приложение №2 к постановлению |
| администрации Чамзинского муниципального района  Республики Мордовия |
| от «\_\_\_» \_\_\_\_ 2019 г. № \_\_ |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в информационной системе «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** информационной системы «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ИС «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п. 6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ИС «Реестр опекаемых детей».

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ИС «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в информационной системе «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в информационной системе Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |
| --- |
| Приложение №3 к постановлению |
| администрации Чамзинского муниципального района  Республики Мордовия |
| от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г. № \_\_ |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в информационной системе «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в информационной системе (далее – ИС) «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **Информационная система «Реестр опекаемых детей»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ИС «Реестр опекаемых детей» Администрации исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства ИС «Реестр опекаемых детей» Администрации располагаются по адресу431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы, д.1.

Информационное взаимодействие в ИС организовано на базе локальных вычислительных сетей, построенных по стандарту IEEE 802.3u. Рабочие станции имеют подключения к информационно-телекоммуникационным сетям международного информационного обмена. Линии связи не выходят за пределы контролируемой зоны.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечением ESET NOT 32.

1. **Расчет показателя исходной защищенности ИС**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации в соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ИС «Реестр опекаемых детей» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В. Г. Цыбаков |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

19.08.2019 г. № 621

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Система исполнения услуг» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Система исполнения услуг» администрации Чамзинского муниципального района

Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Система исполнения услуг» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

3. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Система исполнения услуг» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия  от «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г. № \_\_ |

**Состав и содержание мер защиты информации (базовый набор)**

**для автоматизированной информационной системы «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**ОДЕРЖАНИЕ**

[Обозначения и сокращения 4](#_Toc522787371)

[1. Введение 5](#_Toc522787372)

[2. Требования к мерам защиты информации, содержащейся в АИС «Система исполнения услуг» 5](#_Toc522787373)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 6](#_Toc522787374)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 6](#_Toc522787375)

[3.2. Управление доступом субъектов доступа к объектам доступа 7](#_Toc522787376)

[3.3. Ограничение программной среды 7](#_Toc522787377)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 8](#_Toc522787378)

[3.5. Регистрация событий безопасности 8](#_Toc522787379)

[3.6. Антивирусная защита 8](#_Toc522787380)

[3.7. Контроль (анализ) защищенности информации 9](#_Toc522787381)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc522787382)

[3.9. Защита среды виртуализации 9](#_Toc522787383)

[3.10. Защита технических средств 10](#_Toc522787384)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc522787385)

[4. Состав и содержание компенсирующих мер 11](#_Toc522787386)

[5. Заключение 16](#_Toc522787387)

Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в автоматизированной информационной системе третьего класса защищенности «Система исполнения услуг» (далее – АИС «СИУ») Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в АИС «Система исполнения услуг»

Организационные и технические меры защиты информации, реализуемые в АИС «СИУ» Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г. №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| риложение №2 к постановлению |
| администрации Чамзинского муниципального района  Республики Мордовия |
| от «\_\_\_» \_\_\_\_ 2019 г. № \_\_ |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** автоматизированной информационной системы «Система исполнения услуг» (далее – АИС «СИУ») Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для АИС «СИУ» Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности АИС «СИУ» Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для АИС «СИУ» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в АИС «СИУ» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |
| --- |
| Приложение №3 к постановлению |
| администрации Чамзинского муниципального района Республики Мордовия |
| от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2019 г. № \_\_ |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в автоматизированной информационной системе «Система исполнения услуг» (далее – АИС «СИУ») Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **Система исполнения услуг** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | региональный |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» АИС «СИУ» Администрации Чамзинского района Республики Мордовия исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства АИС «СИУ» Администрации Чамзинского муниципального района Республики Мордовия располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы, д. 1.

Информационное взаимодействие в АИС организовано через сеть СМЭВ. Подключение к сети СМЭВ осуществляется посредством ViPNet.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемKaspersky Endpoint Security 10.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: распределенная ИС, которая охватывает несколько областей, краев, округов или государство в целом. |  |  | + |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + |  |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: модификация и передача |  |  | + |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: интегрированная ИС (организация использует несколько баз ПДн ИС, при этом организация не является владельцем всех используемых баз ПДн); |  |  | + |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 14%\* | 43%\*\* | 57% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **НИЗКАЯ.**

Показатель защищенности **Y1=10**.

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 2  (низкая) | 0,6  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 2  (низкая) | 0,6  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 2  (низкая) | 0,6  (средняя) | | высокая | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 2  (низкая) | 0,6  (средняя) | | высокая | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера** | | | | | | | |
| Утрата ключей доступа | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| 2.4 Угрозы преднамеренных действий внутренних нарушителей | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п. 6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,6  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,6  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для автоматизированной информационной системе «Система исполнения услуг» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых» /предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

ПОСТАНОВЛЕНИЕ

26.09.2019г. № 707

рп. Чамзинка

**О внесении изменений в постановление**

**администрации Чамзинского муниципального района**

**от 19.08.2019 года № 616 «О порядке выявления обстоятельств, свидетельствующих о необходимости оказания детям-сиротам и детям, оставшимся без попечения родителей, лицам из числа детей-сирот и детей, оставшимся без попечения родителей, содействия в преодолении трудной жизненной ситуации, при которых договор найма специализированного жилого помещения заключается на новый пятилетний срок, или отсутствия таких обстоятельств»**

В целях привидения нормативно-правовых актов в соответствие с действующим законодательством, администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

**1.** В пункте 17 Подраздела 4 «Организация деятельности Комиссии» Положения по выявлению обстоятельств, свидетельствующих о необходимости оказания детям-сиротам и детям, оставшимся без попечения родителей, лицам из числа детей-сирот и детей, оставшимся без попечения родителей, содействия в преодолении трудной жизненной ситуации, при которых договор найма специализированного жилого помещения заключается на новый пятилетний срок, или отсутствия таких обстоятельств внести следующие изменения:

- слова «Отдел опеки и попечительства Управления по социальной работе администрации Чамзинского муниципального района» заменить на «Комиссия».

**2.** Настоящее постановление вступает в силу со дня его официального опубликования в информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 763

р.п. Чамзинка

**О подготовке к осенне-зимнему пожароопасному периоду 2019-2020 гг.**

В соответствии с Федеральным Законом РФ от 21.12.1994 года № 69-ФЗ «О пожарной безопасности», Федеральным Законом РФ от 06.10.2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Федеральным Законом РФ от 22.07.2008 года № 123-ФЗ «Технический регламент о требованиях пожарной безопасности», в связи с приближением осенне-зимнего пожароопасного периода, в целях обеспечения пожарной безопасности в границах населенных пунктов, зашиты территорий населенных пунктов и организаций от пожаров, а также создания условий для успешного предупреждения и тушения пожаров и возгораний на территории Чамзинского муниципального района, Администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Рекомендовать Главам городских и сельских поселений:

1.1. В срок до 20.11.2019 года провести проверку противопожарного состояния жилого фонда обратив особое внимание на:

наличие и доступность при пожаротушении источников противопожарного водоснабжения (водоемов, прудов, водонапорных башен);

наличие противопожарного инвентаря и средств первичного пожаротушения;

исправность телефонной связи и звуковой сигнализации для оповещения населения о пожаре;

состояние дорог и проездов, а также наличие указателей размещения водоисточников, улиц, номеров домов и принять меры к устранению недостатков.

1.2. Провести в каждом населенном пункте сходы граждан, на которых необходимо проинструктировать жителей о мерах пожарной безопасности, обсудить с ними:

перечень первоочередных мероприятий по обеспечению пожарной безопасности на зимний период;

порядок участия граждан в добровольной пожарной охране;

порядок приобретения, хранения и использования первичных средств пожаротушения и мотопомп.

1.3. В срок до 20.11.2019 года организовать проведение в населенных пунктах уборки сухой растительности и мусора с дворовых и прилегающих к ним территорий, уборку проводить пожаробезопасным способом, при необходимости произвести опашку границ населенных пунктов. Информацию об объемах выполненных работ предоставить в МКУ Чамзинского муниципального района «Единая дежурно-диспетчерская служба» в срок до 05.12.2019 года.

1.4. В каждом населенном пункте, определить необходимый перечень мероприятий по поддержанию в постоянной готовности источников наружного пожаротушения.

1.5. Определить порядок оповещения и эвакуации жителей из населенных пунктов в случае возникновении крупных пожаров непосредственно в населенных пунктах.

1.6. Провести работу по выявлению расположенных на территориях населенных пунктов бесхозяйных строений, составить соответствующий реестр.

1.7. Продолжить работу профилактических групп из числа работников органов местного самоуправления в целях осуществлении подворового обхода жилого сектора, для проведения инструктажей с населением по соблюдению требований пожарной безопасности. Особое внимание уделить проверке мест проживания многодетных семей, одиноких престарелых и неблагополучных граждан, а также проведению собраний (встреч) с населением, с оформлением соответствующих актов (протоколов).

1.8. Организовать оказание помощи социально-неадаптированным гражданам в соответствие с требованиями пожарной безопасности мест их проживания (ремонт электропроводки и печного отопления).

2. Рекомендовать руководителям с/х предприятий и организаций, крестьянско-фермерским хозяйствам, индивидуальным предпринимателям и гражданам, осуществляющим сельскохозяйственную деятельность:

2.1. Обеспечить выполнение комплекса мер по обеспечению пожарной безопасности и технической укрепленности объектов хранения и переработки грубых кормов. Закладку кормов в хранилища производить только после проведения проверки и принятия решения о соответствии хранилища требованиям пожарной безопасности.

3. Контроль за выполнением настоящего постановления возложить на  
заместителя Главы Чамзинского муниципального района, председателя КЧС и ОПБ Тюрякина А.Ю.

4. Настоящее постановление вступает в силу после его опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 750

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Общероссийский день приема граждан» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Общероссийский день приемаграждан» администрации Чамзинского муниципального района

Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Общероссийский день приемаграждан» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Общероссийский день приемаграждан» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Приложение №1 к постановлению | | администрации Чамзинского муниципального района Республики Мордовия | | от 11.10. 2019 г. № 750 | |

**Состав и содержание мер защиты информации (базовый набор)**

**для информационной системы «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 4](#_Toc520729764)

[1. Введение 5](#_Toc520729765)

[2. Требования к мерам защиты информации, содержащейся в ИС «Общероссийский день приема граждан» 5](#_Toc520729766)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 6](#_Toc520729767)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 6](#_Toc520729768)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc520729769)

[3.3. Ограничение программной среды 7](#_Toc520729770)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc520729771)

[3.5. Регистрация событий безопасности 8](#_Toc520729772)

[3.6. Антивирусная защита 8](#_Toc520729773)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc520729774)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc520729775)

[3.9. Защита среды виртуализации 9](#_Toc520729776)

[3.10. Защита технических средств 10](#_Toc520729777)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc520729778)

[4. Состав и содержание компенсирующих мер 11](#_Toc520729779)

[5. Заключение 15](#_Toc520729780)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в информационной системе (далее – ИС) третьего класса защищенности «Общероссийский день приема граждан» (далее – ОДПГ) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в ИС «Общероссийский день приема граждан»

Организационные и технические меры защиты информации, реализуемые в ИС ОДПГ Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в информационной системе «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия», утвержденной распоряжением администрации Чамзинского муниципального района от 13.08.2019 г №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В информационной системе «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| Приложение № 2 к постановлению |
| администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 750 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в информационной системе «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультант администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** информационной системы (далее – ИС) «Общероссийский день приема граждан» (далее – ОДПГ) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация) с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ИС «ОДПГ» Администрации **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются**. | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2**. **Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ИС ОДПГ Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ИС «ОДПГ» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в информационной системе «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации, подлежащим реализации в информационной системе «ОДПГ» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |
| --- |
| Приложение № 3 к постановлению |
| администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 750 |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в информационной системе «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в информационной системе (далее – ИС) «Общероссийский день приема граждан» (далее – ОДПГ) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **Информационная система «Общероссийский день приема граждан»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ИС «ОДПГ» Администрации исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская.**

Технические средства ИС «ОДПГ» Администрации располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы д.1.

Информационное взаимодействие в ИС Общероссийский день приема граждан» организовано через сеть СМЭВ. Подключение к сети СМЭВ осуществляется посредством ViPNet.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемKaspersky Endpoint Security 10.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ИС «Общероссийский день приема граждан» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В. Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 751

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Единой государственной информационной системы социального обеспечения» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Единой государственной информационной системе социального обеспечения» администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Единой государственной информационной системе социального обеспечения» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Единой государственной информационной системе социального обеспечения» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Приложение №1 к постановлению | | администрации Чамзинского муниципального района Республики Мордовия | | от 11.10. 2019 г. № 751 | |

**Состав и содержание мер защиты информации (базовый набор)**

**для Единой Государственной информационной системы социального обеспечения Администрации Чамзинского муниципального района**

**Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 4](#_Toc520277192)

[1. Введение 5](#_Toc520277193)

[2. Требования к мерам защиты информации, содержащейся в ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия 5](#_Toc520277194)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc520277195)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 6](#_Toc520277196)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc520277197)

[3.3. Ограничение программной среды 7](#_Toc520277198)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc520277199)

[3.5. Регистрация событий безопасности 7](#_Toc520277200)

[3.6. Антивирусная защита 8](#_Toc520277201)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc520277202)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc520277203)

[3.9. Защита среды виртуализации 9](#_Toc520277204)

[3.10. Защита технических средств 9](#_Toc520277205)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc520277206)

[4. Состав и содержание компенсирующих мер 10](#_Toc520277207)

[5. Заключение 15](#_Toc520277208)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в государственной информационной системе третьего класса Единой Государственной информационной системы социального обеспечения (далее – ЕГИССО) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия

Организационные и технические меры защиты информации, реализуемые в ЕГИССО Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в Единой государственной информационной системе социального обеспечения Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от 13 августа 2019 г. №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В информационной системе ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| Приложение №2 к постановлению |
| администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 751 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в Единой Государственной информационной системе социального обеспечения Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальник отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

проведено уточнение адаптированного базового набора мер защиты информации Единой Государственной информационной системе социального обеспечения (далее – ЕГИССО)Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2**. **Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в Единой государственной информационной системе социального обеспечения Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_ \_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |
| --- |
|  |
| Приложение №3 к постановлению |
| администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 751 |
|  |
|  |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в Единой Государственной информационной системе социального обеспечения** **Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в Единой Государственной информационной системе социального обеспечения (далее - ЕГИССО) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **ЕГИССО** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | распределенная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ЕГИССО Администрации Чамзинского района Республики Мордовия исходя из технологий обработки ПДн, целей и состава ПДн определена категория **сегментная**.

Технические средства ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия располагаются по адресу:431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы д.1.

Информационное взаимодействие в ИС организовано на базе локальных вычислительных сетей, построенных по стандарту IEEE 802.3u. Рабочие станции имеют подключения к информационно-телекоммуникационным сетям международного информационного обмена. Линии связи не выходят за пределы контролируемой зоны.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечением ESET NOT 32.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств, внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п. 6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ЕГИССО Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г.Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 752

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в «Государственной информационной системе о государственных и муниципальных платежах» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для «Государственной информационной системы о государственных и муниципальных платежах» администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в «Государственной информационной системе о государственных и муниципальных платежах» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в «Государственной информационной системе о государственных и муниципальных платежах» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района Республики Мордовия  от 11.10. 2019г. № 752 |

**Состав и содержание мер защиты информации (базовый набор)**

**для Государственной информационной системы о государственных и муниципальных платежах Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 4](#_Toc522697734)

[1. Введение 5](#_Toc522697735)

[2. Требования к мерам защиты информации, содержащейся в ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия 5](#_Toc522697736)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc522697737)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 5](#_Toc522697738)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc522697739)

[3.3. Ограничение программной среды 6](#_Toc522697740)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc522697741)

[3.5. Регистрация событий безопасности 7](#_Toc522697742)

[3.6. Антивирусная защита 7](#_Toc522697743)

[3.7. Контроль (анализ) защищенности информации 7](#_Toc522697744)

[3.8. Обеспечение целостности информационной системы и информации 8](#_Toc522697745)

[3.9. Защита среды виртуализации 8](#_Toc522697746)

[3.10. Защита технических средств 8](#_Toc522697747)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 9](#_Toc522697748)

[4. Состав и содержание компенсирующих мер 9](#_Toc522697749)

[5. Заключение 13](#_Toc522697750)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в Государственной информационной системе о государственных и муниципальных платежах (далее ‒ ГИС ГМП) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация) третьего класса защищенности.

# 2. Требования к мерам защиты информации, содержащейся в ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия

Организационные и технические меры защиты информации, реализуемые в ГИС ГМП Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в Государственной информационной системе о государственных и муниципальных платежах Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г. №234 «Об утверждении документов по защите информации.

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
|  |
| Приложение №2 к постановлению  администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 752 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в Государственной информационной системе о государственных и муниципальных платежах Администрации Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** Государственной информационной системы о государственных и муниципальных платежах (далее – ГИС ГМП) Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в Государственной информационной системе о государственных и муниципальных платежах Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |

|  |
| --- |
|  |
| Приложение №3 к постановлению  администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 752 |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в Государственной информационной системе о государственных и муниципальных платежах Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в Государственной информационной системе о государственных и муниципальных платежах (далее ‒ ГИС ГМП) Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **ГИС ГМП** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ГИС ГМП Администрации Чамзинского района Республики Мордовия исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия располагаются по адресу431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы, д.1.

Информационное взаимодействие с другими участниками ГИС ГМП организовано через сеть СМЭВ. Подключение к сети СМЭВ осуществляется посредством ViPNet.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемESET NOT 32.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: модфикация и передача |  |  | + |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 43%\* | 71%\*\* | 29% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п. 6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ГИС ГМП Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 753

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в автоматизированной информационной системе «Сельское административное образование» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системе «Сельское административное образование» администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Сельское административное образование» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Сельское административное образование» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района Республики Мордовия  от 11.10. 2019 г. № 753 |

**Состав и содержание мер защиты информации (базовый набор)**

**для автоматизированной информационной системы «Сельское административное образование» Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 3](#_Toc520453436)

[1. Введение 4](#_Toc520453437)

[2. Требования к мерам защиты информации, содержащейся в АИС «САО» 4](#_Toc520453438)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc520453439)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 5](#_Toc520453440)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc520453441)

[3.3. Ограничение программной среды 7](#_Toc520453442)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc520453443)

[3.5. Регистрация событий безопасности 7](#_Toc520453444)

[3.6. Антивирусная защита 8](#_Toc520453445)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc520453446)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc520453447)

[3.9. Защита среды виртуализации 9](#_Toc520453448)

[3.10. Защита технических средств 9](#_Toc520453449)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc520453450)

[4. Состав и содержание компенсирующих мер 10](#_Toc520453451)

[5. Заключение 16](#_Toc520453452)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в информационной системе третьего класса защищенности «Сельское административное образование» (далее – АИС «САО») Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в АИС «САО»

Организационные и технические меры защиты информации, реализуемые в АИС «САО» Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в автоматизированной информационной системе «Сельское административное образование» Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г. №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
|  |
| Приложение №2 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия |
| от 11.10. 2019 г. № 753 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в автоматизированной информационной системе «Сельское**

**административное образование» Администрации Чамзинского**

**муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** автоматизированной информационной системы «Сельское административное образование» (далее – АИС «САО») Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| 2.5 Угрозы несанкционированного доступа по каналам связи | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |

|  |
| --- |
|  |
| приложение №3 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия |
| от 11.10. 2019 г. № 753 |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке в автоматизированной информационной системе «Сельское административное образование»**

**Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в автоматизированной информационной системе «Сельское административное образование» (далее – АИС «САО») Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **АИС «САО»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» АИС «САО» Администрации исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства АИС «САО» Администрации располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы, д.1.

Информационное взаимодействие в ИС организовано на базе локальных вычислительных сетей, построенных по стандарту IEEE 802.3u. Рабочие станции имеют подключения к информационно-телекоммуникационным сетям международного информационного обмена. Линии связи не выходят за пределы контролируемой зоны.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечением ESET NOT 32.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п. 6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для АИС «САО» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 754

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в автоматизированной информационной системе «Несовершеннолетние и семьи»» администрации Чамзинского муниципального района Республики Мордовия**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для автоматизированной информационной системы «Несовершеннолетние и семьи» администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в автоматизированной информационной системе «Несовершеннолетние и семьи» администрации Чамзинского муниципального района Республики Мордовия (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в автоматизированной информационной системе «Несовершеннолетние и семьи» администрации Чамзинского муниципального района Республики Мордовия (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия  от 11.10.2019 г. № 754 |

**Состав и содержание мер защиты информации (базовый набор)**

**для автоматизированной информационной системы «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 3](#_Toc522629482)

[1. Введение 4](#_Toc522629483)

[2. Требования к мерам защиты информации, содержащейся в АИС «Несовершеннолетние и семьи» 4](#_Toc522629484)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc522629485)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 5](#_Toc522629486)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc522629487)

[3.3. Ограничение программной среды 7](#_Toc522629488)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc522629489)

[3.5. Регистрация событий безопасности 7](#_Toc522629490)

[3.6. Антивирусная защита 8](#_Toc522629491)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc522629492)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc522629493)

[3.9. Защита среды виртуализации 9](#_Toc522629494)

[3.10. Защита технических средств 9](#_Toc522629495)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc522629496)

[4. Состав и содержание компенсирующих мер 10](#_Toc522629497)

[5. Заключение 16](#_Toc522629498)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в автоматизированной информационной системе третьего класса защищенности «Несовершеннолетние и семьи» (далее – АИС «Несовершеннолетние и семьи») Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация).

# 2. Требования к мерам защиты информации, содержащейся в АИС «Несовершеннолетние и семьи»

Организационные и технические меры защиты информации, реализуемые в АИС «Несовершеннолетние» Администрации рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в автоматизированной информационной системе «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия, утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
| Приложение №2 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия |
| от 11.10. 2019 г. № 754 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в автоматизированной информационной системе**

**«Несовершеннолетние и семьи» Администрации**

**Чамзинского муниципального района Республики Мордовия.**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии:

Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** автоматизированной информационной системы «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в автоматизированной информационной системе «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в и автоматизированной информационной системе «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия» класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |

|  |
| --- |
| Приложение №3 к постановлению  администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 754 |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке в автоматизированной информационной системе «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в автоматизированной информационной системе «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия (далее – Администрация), а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **АИС «Несовершеннолетние и семьи»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» АИС «Несовершеннолетние и семьи» Администрации Чамзинского района Республики Мордовия исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы д.1.

Информационное взаимодействие в АИС осуществляется по защищенному каналу посредством OpenVPN. На рабочих станциях АИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемKaspersky Endpoint Security 10.

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 7.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для АИС «Несовершеннолетние и семьи» Администрации Чамзинского муниципального района Республики Мордовия актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых»/предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г.Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

Администрация Чамзинского муниципального района

Республики Мордовия

**ПОСТАНОВЛЕНИЕ**

11.10.2019 г. № 755

р.п. Чамзинка

**Об утверждении нормативно-правовых актов в сфере защиты персональных данных при их обработке в информационной системе «Администрация Чамзинского муниципального района**

**Республики Мордовия».**

В целях исполнения Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», администрация Чамзинского муниципального района

**ПОСТАНОВЛЯЕТ:**

1. Утвердить состав и содержание мер защиты информации (базовый набор) для информационной системы «Администрация Чамзинского муниципального района Республики Мордовия» третьего класса защищенности (приложение №1).

2. Утвердить акт уточнения адаптированного базового набора мер защиты информации в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» (приложение №2).

3. Утвердить модель угроз безопасности информации ограниченного доступа прав при ее обработке в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» (приложение №3).

4. Настоящее постановление вступает в силу со дня его официального опубликования в Информационном бюллетене Чамзинского муниципального района.

Глава Чамзинского муниципального района В.Г. Цыбаков

|  |
| --- |
| Приложение №1 к постановлению  администрации Чамзинского муниципального района  Республики Мордовия  от 11.10. 2019 г. № 755 |

**Состав и содержание мер защиты информации (базовый набор)**

**для информационной системы «Администрация Чамзинского муниципального района Республики Мордовия» третьего класса защищенности**

**СОДЕРЖАНИЕ**

[Обозначения и сокращения 3](#_Toc520277192)

[1. Введение 4](#_Toc520277193)

[2. Требования к мерам защиты информации, содержащейся в ИС «Администрация Чамзинского муниципального района Республики Мордовия» 4](#_Toc520277194)

[3. Состав и содержание базовых мер по обеспечению безопасности информации 5](#_Toc520277195)

[3.1. Идентификация и аутентификация субъектов доступа и объектов доступа 5](#_Toc520277196)

[3.2. Управление доступом субъектов доступа к объектам доступа 6](#_Toc520277197)

[3.3. Ограничение программной среды 6](#_Toc520277198)

[3.4. Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация 7](#_Toc520277199)

[3.5. Регистрация событий безопасности 7](#_Toc520277200)

[3.6. Антивирусная защита 8](#_Toc520277201)

[3.7. Контроль (анализ) защищенности информации 8](#_Toc520277202)

[3.8. Обеспечение целостности информационной системы и информации 9](#_Toc520277203)

[3.9. Защита среды виртуализации 9](#_Toc520277204)

[3.10. Защита технических средств 9](#_Toc520277205)

[3.11. Защита информационной системы, ее средств, систем связи и передачи данных 10](#_Toc520277206)

[4. Состав и содержание компенсирующих мер 10](#_Toc520277207)

[5. Заключение 16](#_Toc520277208)

# Обозначения и сокращения

|  |  |
| --- | --- |
| ИАФ | Идентификация и аутентификация субъектов доступа и объектов доступа |
| УПД | Управление доступом субъектов доступа к объектам доступа |
| ОПС | Ограничение программной среды |
| ЗНИ | Защита машинных носителей информации |
| РСБ | Регистрация событий безопасности |
| АВЗ | Антивирусная защита |
| СОВ | Обнаружение вторжений |
| АНЗ | Контроль (анализ) защищенности информации |
| ОЦЛ | Обеспечение целостности информационной системы и информации |
| ОДТ | Обеспечение доступности информации |
| ЗСВ | Защита среды виртуализации |
| ЗТС | Защита технических средств |
| ЗИС | Защита информационной системы, ее средств, систем связи и передачи данных |
| ИНЦ | Выявление инцидентов и реагирование на них |
| УКФ | Управление конфигурацией информационной системы и системы защиты информации |

# 1. Введение

Меры по обеспечению безопасности информации принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также от иных неправомерных действий в отношении информации.

В данном документе представлен состав и содержание **базовых** мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, обрабатываемых в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» третьего класса защищенности

# 2. Требования к мерам защиты информации, содержащейся в ИС «Администрация Чамзинского муниципального района Республики Мордовия»

Организационные и технические меры защиты информации, реализуемые в ИС «Администрация Чамзинского муниципального района Республики Мордовия» рамках построения системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* контроль (анализ) защищенности информации;
* целостность информационной системы и информации;
* защиту среды виртуализации;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

* определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
* адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
* дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты информации.

# 3. Состав и содержание базовых мер по обеспечению безопасности информации

Базовый набор мер защиты информации для информационной системы для третьего класса защищенности определен в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также в соответствии с «Моделью угроз безопасности информации ограниченного доступа при их обработке в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия», утвержденной распоряжением администрации Чамзинского муниципального района от «13» августа 2019 г. №234 «Об утверждении документов по защите информации».

## Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |

## Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |

## Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОПС.З | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |

## Защита машинных носителей информации, на которых хранится и (или) обрабатывается информация

Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |

## Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.З | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |

## Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АВ3.1 | Реализация антивирусной защиты |
| АВ3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

## Контроль (анализ) защищенности информации

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

## Обеспечение целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |

## Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |

## Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

## Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

| **Номер и условное обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

# 4. Состав и содержание компенсирующих мер

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» определены следующие состав и содержание компенсирующих мер защиты информации для информационной системы третьего класса защищенности.

| **Номер и условное**  **обозначение меры** | **Меры по обеспечению безопасности информации** |
| --- | --- |
|
| **Идентификация и аутентификация субъектов доступа и объектов доступа** | |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных |
| ИАФ.7 | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа |
| **Управление доступом субъектов доступа к объектам доступа** | |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы Меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |
| **Ограничение программной среды** | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов |
| **Защита машинных носителей информации** | |
| ЗНИ.З | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| **Регистрация событий безопасности** | |
| РСБ.8 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе |
| **Обнаружение вторжений** | |
| СОВ.1 | Обнаружение вторжений |
| СОВ.2 | Обновление базы решающих правил |
| **Обеспечение целостности информационной системы и информации** | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации |
| ОЦЛ.2 | Контроль целостности информации, содержащейся в базах данных информационной системы |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) |
| ОЦЛ. 5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |
| **Обеспечение доступности информации** | |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| ОДТ.4 | Периодическое резервное копирование информации на резервные машинные носители информации |
| ОДТ.5 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала |
| ОДТ.6 | Кластеризация информационной системы и (или) ее сегментов |
| ОДТ.7 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации |
| **Защита среды виртуализации** | |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигурации |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| **Защита технических средств** | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) |
| **Защита информационной системы, ее средств, систем связи и передачи данных** | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными информационными системами |
| ЗИС. 7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода |
| ЗИС. 8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |
| ЗИС.21 | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы |
| ЗИС.22 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы |
| ЗИС.23 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации |
| ЗИС.28 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы |
| ЗИС.29 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы |

В случае обработки в информационной системе информации, содержащей персональные данные, для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для 3 и 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1. организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. обеспечение сохранности носителей персональных данных;
3. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

# 5. Заключение

В информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» должен быть, как минимум, реализован адаптированный базовый набор мер защиты информации, соответствующий установленному классу защищенности информационной системы.

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

В этом случае в ходе разработки системы защиты информации информационной системы должно быть проведено обоснование применения компенсирующих мер защиты информации, а при аттестационных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

|  |
| --- |
|  |
| Приложение №2 к постановлению  администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019г. № 755 |

**АКТ УТОЧНЕНИЯ**

**адаптированного базового набора мер защиты информации**

**в информационной системе «Администрация Чамзинского**

**муниципального района Республики Мордовия».**

**Введение**

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

1. **Уточнение адаптированного базового набора мер защиты информации информационной системы**

Комиссией, назначенной распоряжением администрации Чамзинского муниципального района от 06.09.2018 г. № 188 «О защите персональных данных» в составе председателя комиссии: Руководителя аппарата администрации Чамзинского муниципального района ‒ Настиной Светланы Михайловны,

членов комиссии:

Долгова В.И. – начальника отдела специальных программ администрации Чамзинского муниципального района;

Казаковой М.В. – начальника отдела информатизации администрации Чамзинского муниципального района;

Додайкиной Н.М. – консультанта администрации Чамзинского муниципального района

**проведено уточнение адаптированного базового набора мер защиты информации** информационной системы «Администрация Чамзинского муниципального района Республики Мордовия» с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы, в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставлялась мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы.

В случае, если адаптированный базовый набор мер защиты информации не обеспечивал блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включались меры защиты информации, приведенные в разделе 3 методического документа ФСТЭК России от 11 февраля 2014 «Меры защиты информации в государственных информационных системах».

При этом содержание данной меры защиты информации определялось с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

В таблице 1 представлен адаптированный базовый набор мер защиты информации, обеспечивающий блокирование угроз безопасности или снижающий вероятность их реализации исходя из условий функционирования информационной системы, сопоставленный с угрозами безопасности информации, включенными в модель угроз для ИС «Администрация Чамзинского муниципального района Республики Мордовия» **класса защищенности К3**.

Таблица 1

| **Наименование угрозы** | **Меры защиты информации** | **Адаптированный**  **базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| --- | --- | --- | --- |
| 1. **Угрозы утечки информации по техническим каналам** | | | |
| **1.1 Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | |
| **1.2 Угрозы утечки видовой информации** | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | ИАФ.5 | **+** | **+** |
| УПД.10 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| **1.3 Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 6.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | |
| **2.1 Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | |
| Кража ПЭВМ | АНЗ.4 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Кража носителей информации | УПД.15 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **-** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Модификация и уничтожение информации. | ОДТ.5 | **-** | **+** |
| ЗИС.3 | **+** | **+** |
| ЗИС.7 | **+** | **+** |
| Вывод из строя узлов ПЭВМ, каналов связи | АНЗ.4 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | ИАФ.1 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) | | | |
| Угроза внедрения вредоносных программ | ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| Перехват паролей, идентификаторов при входе в систему | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| 2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | | |
| Утрата ключей доступа | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| Выход из строя аппаратно-программных средств | АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Сбой системы электроснабжения | ОЦЛ.1 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ОДТ.3 | **+** | **+** |
| ОДТ.4 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| ЗТС.5 | **+** | **+** |
| 2.4 Угрозы преднамеренных действий внутренних нарушителей | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | ИАФ.1 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.10 | **+** | **+** |
| УПД.14 | **+** | **+** |
| УПД.15 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **-** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.6 | **-** | **+** |
| ЗНИ.7 | **-** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | УПД.1 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| ЗИС.30 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ОДТ.5 | **+** | **+** |
| 2.5 Угрозы несанкционированного доступа по каналам связи | | | |
| Угрозы внедрения по сети вредоносных программ | УПД.16 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| 2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | УПД.13 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | |
| Угроза несанкционированного изменения аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| **4. Угрозы нарушения доступности информации** | | | |
| Угроза повреждения системного реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза вывода из строя/выхода из строя отдельных ТС | ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ОДТ.1 | **-** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.5 | **-** | **+** |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | АНЗ.3 | + | + |
| ОЦЛ.3 | + | + |
| АВЗ.1 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.1 | - | + |
| ОДТ.3 | - | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| ЗИС.3 | - | + |
| ЗИС.11 | - | + |
| ЗИС.23 | - | + |
| **5. Угрозы нарушения целостности информации** | | | |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | УПД.2 | - | + |
| ОЦЛ.3 | + | + |
| ОЦЛ.4 | - | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ЗИС.1 | - | + |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза передачи из ИС недопустимой информации | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| АНЗ.1 | + | + |
| ОЦЛ.3 | + | + |
| Угроза подмены используемых ИС файлов | ИАФ.1 | - | + |
| ИАФ.3 | + | + |
| ИАФ.4 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.11 | + | + |
| ЗНИ.1 | + | + |
| ЗНИ.3 | + | + |
| ЗНИ.5 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.4 | - | + |
| ОДТ.5 | - | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АНЗ.3 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.3 | + | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ОДТ.5 | - | + |
| **6. Угрозы, не являющиеся атаками** | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | ОДТ.1 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | |
| Угроза аппаратного сброса пароля BIOS | ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза обхода некорректно настроенных механизмов аутентификации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| Угроза программного сброса пароля BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ЗИС.3 | **+** | **+** |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.11 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования «слабых»/предсказуемых паролей | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Угроза отсутствия регламента работы с персональными идентификаторами | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **-** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **-** | **+** |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | |
| Угроза доступа к защищаемым файлам с использованием обходного пути | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза загрузки нештатной ОС | УПД.15 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза использования альтернативных путей доступа к ресурсам | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного доступа к аутентификационной информации | ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза несанкционированного копирования защищаемой информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| ЗНИ.6 | **+** | **+** |
| ЗНИ.7 | **+** | **+** |
| ЗНИ.8 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза несанкционированного редактирования реестра | УПД.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОДТ.4 | **-** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| Угроза несанкционированного создания учётной записи пользователя | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | УПД.4 | **+** | **+** |
| ОДТ.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза удаления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **-** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования незавершенных сеансов пользователей | УПД.10 | **+** | **+** |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **-** | **+** |
| ОДТ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | УПД.1 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.3 | **-** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Хищение ключей шифрования, идентификаторов и известных паролей | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| ИАФ.6 | **-** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| УПД.11 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Несанкционированное отключение средств защиты | УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| **11. Угрозы нарушения конфиденциальности** | | | |
|  | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| Угроза получения предварительной информации об объекте защиты | УПД.4 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| ЗТС.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| **12. Угрозы программно-математических воздействий** | | | |
| Угроза внедрения кода или данных | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза восстановления аутентификационной информации | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | - | + |
| ИАФ.5 | + | + |
| УПД.4 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| АНЗ.5 | + | + |
| ЗИС.1 | + | + |
|  | **+** | **+** |
| Угроза деструктивного изменения конфигурации/среды окружения программ | АНЗ.2 | **+** | **+** |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | ЗТС.2 | **+** | **+** |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | АВЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза неправомерного шифрования информации | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза распространения «почтовых червей» | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Внедрение программных закладок | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Применение специально созданных программных продуктов для НСД | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| ЗИС.1 | **-** | **+** |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| Отсутствие централизованной системы управления средствами антивирусной защиты | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ЗНИ.8 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного удаления защищаемой информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **-** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| Угроза утраты носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Угроза форматирования носителей информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Повреждение носителя информации | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза подключения к ИС неучтенных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза подключения к ИС неперсонифицированных машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного копирования информации на машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| ИАФ.4 | **+** | **+** |
| ИАФ.5 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза хищения машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза подмены машинных носителей | ЗТС.2 | **+** | **+** |
| ОДТ.4 | **-** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗНИ.5 | **+** | **+** |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| Угроза несанкционированного использования машинных носителей | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | + | + |
| ЗТС.3 | + | + |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | |
| Угроза внедрения вредоносного кода в BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза изменения компонентов системы | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.4 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| ОПС.1 | **-** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.1 | **-** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ОДТ.5 | **-** | **+** |
| Угроза ошибочного запуска/установки программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| **16. Угрозы физического доступа к компонентам ИС** | | | |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | ЗТС.2 | **+** | **+** |
| Угроза нарушение функционирования НЖМД и других систем хранения данных | ЗНИ.1 | **+** | **+** |
| ЗНИ.2 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| ЗТС.3 | **+** | **+** |
| Отсутствие средств автоматизированного контроля доступа | ЗТС.2 | **+** | **+** |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | |
| Угроза восстановления предыдущей уязвимой версии BIOS | ИАФ.1 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **-** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.2 | **-** | **+** |
| ОПС.3 | **+** | **+** |
| АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза деструктивного использования декларированного функционала BIOS | УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ЗИС.1 | **+** | **+** |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |
| ЗТС.2 | **+** | **+** |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | АВЗ.1 | **+** | **+** |
| АВЗ.2 | **+** | **+** |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | ЗИС.3 | **+** | **+** |
| Угроза отсутствия проверки подлинности сетевых соединений | ЗИС.3 | + | + |
| **19. Угрозы инженерной инфраструктуры** | | | |
| Угрозы сбоев в сети электропитания | ОДТ.1 | **+** | **+** |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми событиями | РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.5 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза переполнения журналов информационной безопасности | РСБ.1 | **+** | **+** |
| РСБ.2 | **+** | **+** |
| РСБ.3 | **+** | **+** |
| РСБ.4 | **+** | **+** |
| РСБ.6 | **+** | **+** |
| РСБ.7 | **+** | **+** |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | РСБ.1 | + | + |
| РСБ.2 | + | + |
| Угроза модификации/удаления журнала информационной безопасности | ИАФ.1 | + | + |
| ИАФ.3 | + | + |
| УПД.1 | + | + |
| УПД.2 | + | + |
| УПД.4 | + | + |
| УПД.5 | + | + |
| УПД.6 | + | + |
| АВЗ.1 | + | + |
| АВЗ.2 | + | + |
| РСБ.1 | + | + |
| РСБ.2 | + | + |
| РСБ.3 | + | + |
| РСБ.5 | + | + |
| РСБ.6 | + | + |
| РСБ.7 | + | + |
| ОПС.1 | - | + |
| ОПС.2 | - | + |
| ОПС.4 | - | + |
| ОЦЛ.1 | - | + |
| ОЦЛ.3 | + | + |
| ЗИС.3 | - | + |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | ИАФ.1 | **+** | **+** |
| ИАФ.3 | **+** | **+** |
| УПД.1 | **+** | **+** |
| УПД.2 | **+** | **+** |
| УПД.4 | **+** | **+** |
| УПД.5 | **+** | **+** |
| УПД.6 | **+** | **+** |
| ОПС.3 | **+** | **+** |
| АНЗ.5 | **+** | **+** |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | ОПС.3 | **+** | **+** |
| АНЗ.1 | **+** | **+** |
| АНЗ.2 | **+** | **+** |
| АНЗ.3 | **+** | **+** |
| ОЦЛ.3 | **+** | **+** |

В таблице 2 представлены меры защиты информации, не входящие в состав базового набора мер защиты информации для выбранного класса, а также меры, входящие в базовый набор мер защиты информации для класса защищенности **К3** не обеспечивающие нейтрализацию актуальных угроз иреализуемые для усиления общей защищенности ИС «Администрация Чамзинского муниципального района Республики Мордовия.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры защиты информации** | **Набор мер защиты информации** | | |
| **Базовый** | **Адаптированный** | **Уточненный** |
| УПД.11 | + | + | + |
| УПД.17 | - | - | - |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ОДТ.5 | - | - | + |

В таблице 3 представлен уточненный адаптированный базовый набор мер защиты информации для ИС «Администрация Чамзинского муниципального района Республики Мордовия» класса защищенности К3.

Таблица 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Мера защиты информации** | **Базовый набор мер защиты информации** | **Адаптированный базовый набор мер защиты информации** | **Уточненный адаптированный базовый набор мер защиты информации** |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | |
| ИАФ.1 | + | + | + |
| ИАФ.2 | - | - | - |
| ИАФ.3 | + | + | + |
| ИАФ.4 | + | + | + |
| ИАФ.5 | + | + | + |
| ИАФ.6 | + | Присутствие внешних пользователей не свойственно для ИС | - |
| ИАФ.7 | - | - | - |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | | |
| УПД.1 | + | + | + |
| УПД.2 | + | + | + |
| УПД.3 | - | - | - |
| УПД.4 | + | + | + |
| УПД.5 | + | + | + |
| УПД.6 | + | + | + |
| УПД.7 | - | - | - |
| УПД.8 | - | - | - |
| УПД.9 | - | - | - |
| УПД.10 | + | + | + |
| УПД.11 | + | + | + |
| УПД.12 | - | - | - |
| УПД.13 | + | + | + |
| УПД.14 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| УПД.15 | + | + | + |
| УПД.16 | + | + | + |
| УПД.17 | - | - | - |
| **III. Ограничение программной среды (ОПС)** | | | |
| ОПС.1 | - | - | + |
| ОПС.2 | - | - | + |
| ОПС.3 | + | + | + |
| ОПС.4 | - | - | + |
| **IV. Защита машинных носителей информации (ЗНИ)** | | | |
| ЗНИ.1 | + | + | + |
| ЗНИ.2 | + | + | + |
| ЗНИ.3 | - | - | + |
| ЗНИ.4 | - | - | - |
| ЗНИ.5 | - | - | + |
| ЗНИ.6 | - | - | + |
| ЗНИ.7 | - | - | + |
| ЗНИ.8 | + | + | + |
| **V. Регистрация событий безопасности (РСБ)** | | | |
| РСБ.1 | + | + | + |
| РСБ.2 | + | + | + |
| РСБ.3 | + | + | + |
| РСБ.4 | + | + | + |
| РСБ.5 | + | + | + |
| РСБ.6 | + | + | + |
| РСБ.7 | + | + | + |
| РСБ.8 | - | - | + |
| **VI. Антивирусная защита (АВЗ)** | | | |
| АВЗ.1 | + | + | + |
| АВЗ.2 | + | + | + |
| **VII. Обнаружение вторжений (СОВ)** | | | |
| СОВ.1 | - | - | - |
| СОВ.2 | - | - | - |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | | |
| АНЗ.1 | + | + | + |
| АНЗ.2 | + | + | + |
| АНЗ.3 | + | + | + |
| АНЗ.4 | + | + | + |
| АНЗ.5 | + | + | + |
| **IX. Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | |
| ОЦЛ.1 | - | - | + |
| ОЦЛ.2 | - | - | - |
| ОЦЛ.3 | + | + | + |
| ОЦЛ.4 | - | - | + |
| ОЦЛ.5 | - | - | - |
| ОЦЛ.6 | - | - | - |
| ОЦЛ.7 | - | - | - |
| ОЦЛ.8 | - | - | - |
| **X. Обеспечение доступности информации (ОДТ)** | | | |
| ОДТ.1 | - | - | - |
| ОДТ.2 | - | - | - |
| ОДТ.3 | - | - | + |
| ОДТ.4 | - | - | + |
| ОДТ.5 | - | - | + |
| ОДТ.6 | - | - | - |
| ОДТ.7 | - | - | - |
| **XI. Защита среды виртуализации (ЗСВ)** | | | |
| ЗСВ.1 | + | Технология виртуализации не свойственна для ИС | - |
| ЗСВ.2 | + |
| ЗСВ.3 | + |
| ЗСВ.4 | - |
| ЗСВ.5 | - |
| ЗСВ.6 | - |
| ЗСВ.7 | - |
| ЗСВ.8 | - |
| ЗСВ.9 | + |
| ЗСВ.10 | - |
| **XII. Защита технических средств (ЗТС)** | | | |
| ЗТС.1 | - | - | - |
| ЗТС.2 | + | + | + |
| ЗТС.3 | + | + | + |
| ЗТС.4 | + | + | + |
| ЗТС.5 | - | - | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)** | | | |
| ЗИС.1 | - | - | + |
| ЗИС.2 | - | - | - |
| ЗИС.3 | + | + | + |
| ЗИС.4 | - | - | - |
| ЗИС.5 | + | Использование периферийных устройств не свойственно для ИС | - |
| ЗИС.6 | - | - | - |
| ЗИС.7 | - | Технология мобильного кода не свойственна для ИС | - |
| ЗИС.8 | - | Технология передачи речи не свойственна для ИС | - |
| ЗИС.9 | - | Технология передачи видеоинформации не свойственна для ИС | - |
| ЗИС.10 | - | - | - |
| ЗИС.11 | - | - | + |
| ЗИС.12 | - | - | - |
| ЗИС.13 | - | - | - |
| ЗИС.14 | - | - | - |
| ЗИС.15 | - | - | - |
| ЗИС.16 | - | - | - |
| ЗИС.17 | - | - | - |
| ЗИС.18 | - | - | - |
| ЗИС.19 | - | - | - |
| ЗИС.20 | + | Использование технологий беспроводного доступа не свойственно для ИС | - |
| ЗИС.21 | - | - | - |
| ЗИС.22 | - | - | - |
| ЗИС.23 | - | - | + |
| ЗИС.24 | - | - | - |
| ЗИС.25 | - | - | - |
| ЗИС.26 | - | - | - |
| ЗИС.27 | - | - | - |
| ЗИС.28 | - | - | - |
| ЗИС.29 | - | - | - |
| ЗИС.30 | + | + | + |

**Вывод**

Уточненный адаптированный базовый набор мер, представленный в таблице 3, обеспечивающий блокирование (нейтрализацию) всех угроз безопасности информации представленных в «Модели угроз безопасности информации ограниченного доступа при ее обработке в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» является итоговым набором мер защиты информации подлежащим реализации в информационной системе «Администрация Чамзинского муниципального района Республики Мордовия» класса защищенности **К3** в соответствии сразделом 3 методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». Дополнение и применение компенсирующих мер защиты информации не требуется.

|  |  |  |
| --- | --- | --- |
| Председатель: | | \_\_\_\_\_\_\_\_\_\_\_Настина С.М.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
| Члены комиссии: | | \_\_\_\_\_\_\_\_\_\_Казакова М.В.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Долгов В.И.\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_Додайкина Н.М.\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (фамилия, инициалы) (подпись) |
|  |  |  |

|  |
| --- |
|  |
| Приложение №3 к постановлению  администрации Чамзинского муниципального района Республики Мордовия |
| от 11.10. 2019 г. № 755 |

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ**

**информации ограниченного доступа при ее обработке**

**в информационной системе «Администрация Чамзинского**

**муниципального района Республики Мордовия»**

1. **Источники разработки**

Разработка настоящей Модели угроз безопасности, актуализация угроз безопасности информации ограниченного доступа (в том числе и ПДн) и информационных технологий, используемых в информационной системе (далее – ИС) «Администрация Чамзинского муниципального района Республики Мордовия», а также оценка исходной защищенности ИС проведена в соответствии со следующими нормативно-методическим документами:

* 1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
  2. Постановление Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  3. Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).
  4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).
  5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
  6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
  7. Постановление Правительства Республики Мордовия от 07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1. **Описание ИС**

Обобщенные исходные данные по ИС сведены в таблицу.

|  |  |
| --- | --- |
| **Информационная система «Администрация Чамзинского муниципального района Республики Мордовия»** | |
| Исходные данные ИС | |
| Категория ПДн | иная категория ПДн |
| Объем обрабатываемых ПДн | менее 100000 (субъекты ПДн) |
| Структура ИС | локальная ИС |
| Наличие соединений с сетями общего пользования | одноточечное |
| Режим обработки ПДн | многопользовательский |
| Разграничение прав доступа | с разграничением |
| Степень возможного ущерба | низкая |
| Уровень значимости информации | низкий (УЗ 3) |
| Уровень защищенности ПДн | УЗ 4 |
| Масштаб ИС | объектовый |
| Угрозы безопасности | тип 3 |
| Класс защищенности | К3 с необходимостью обеспечения 3-го и 4-го уровня защищенности ПДн |

В соответствии с Постановлением Правительства Республики Мордовия от07 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» ИС «Администрация Чамзинского района Республики Мордовия» исходя из технологий обработки ПДн, целей и состава ПДн определена категория **внутриреспубликанская**.

Технические средства ИС «Администрация Чамзинского муниципального района Республики Мордовия» располагаются по адресу 431700, Республика Мордовия, Чамзинский район, п. Чамзинка, ул. Победы, д. 1 на 1-ом и 2-ом этажах здания Администрации.

Информационное взаимодействие в ИС организовано на базе локальных вычислительных сетей, построенных по стандарту IEEE 802.3u. Рабочие станции имеют подключения к информационно-телекоммуникационным сетям международного информационного обмена. Линии связи не выходят за пределы контролируемой зоны.

На рабочих станциях ИС установлены операционные системы семейства Microsoft Windows с антивирусным программным обеспечениемESET NON 32

1. **Расчет показателя исходной защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС (Y1). В таблице представлены характеристики уровня исходной защищенности.

|  |  |  |  |
| --- | --- | --- | --- |
| **Технические и эксплуатационные характеристики ИС** | **Уровень защищенности** | | |
| Высокий  (В) | Средний  (С) | Низкий  (Н) |
| 1. По территориальному размещению: локальная ИС, развернутая в пределах одного здания; | + |  |  |
| 2. По наличию соединения с сетями общего пользования: ИС, имеющая одноточечный выход в сеть общего пользования; |  | + | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка; |  | + |  |
| 4. По разграничению доступа к персональным данным: ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн; |  | + |  |
| 5. По наличию соединений с другими базами ПДн иных ИС: ИС, в которой используется одна база данных ПДн, принадлежащая организации - владельцу данной ИС; | + |  |  |
| 6. По уровню (обезличивания) ПДн: ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн); |  |  | + |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: ИС, не предоставляющие никакой информации; | + |  |  |
|  | 0,43%\* | 0,85%\*\* | 0,15% |

\* В/7;

\*\* (В+С)/7

*Примечание:*

|  |  |
| --- | --- |
| **Высокий** уровень исходной защищенности | не менее 70% характеристик соответствуют уровню «высокий», а остальные – среднему |
| **Средний** уровень исходной защищенности | не выполняются условия по п. 1 и не менее 70% характеристик соответствуют уровню не ниже «средний» |
| **Низкий** уровень исходной защищенности | не выполняются условия по пунктам 1 и 2 |

Исходная степень защищенности информационной системы персональных данных: **СРЕДНЯЯ**

Показатель защищенности Y1=5

Под вероятностью реализации угрозы (Y2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИС.

|  |  |  |  |
| --- | --- | --- | --- |
| Справочно: | | | |
|  | | | |
| Показатель защищенности  **Y1**  0 для В≥70% при Н=0  5 для В+С≥70%  10 в остальных случаях | Вероятность реализации **Y2**  0 для маловероятной угрозы;  2 для низкой вероятности угрозы;  5 для средней вероятности угрозы;  10 для высокой вероятности угрозы. | Коэффициент реализуемости  угрозы  Y = (Y1 + Y2)/20. | Возможность реализации  угрозы  0 < Y < 0,3 – низкая;  0,3 < Y < 0,6 – средняя;  0,6 < Y < 0,8 – высокая;  Y > 0,8 – очень высокая. |

Правила отнесения угрозы безопасности к актуальной.

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность  реализации угрозы  (Y) | Показатель опасности угрозы  (экспертная оценка) | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

| **Наименование угрозы** | **Вероятность реализации угрозы (Y2)** | **Возможность реализации угрозы (Y)** | | **Опасность угрозы** | **Актуальность угрозы** | **Меры по противодействию угроз** | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Технические** | **Организационные** |
| 1. **Угрозы утечки информации по техническим каналам** | | | | | | | |
| * 1. **Угрозы утечки акустической (речевой) информации – В ИС отсутствуют функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами.** | | | | | | | |
| * 1. **Угрозы утечки видовой информации** | | | | | | | |
| Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн | 5  (средняя) | 0,5 | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Контроль доступа в помещения ИС, расположение технических средств |
| Просмотр информации с помощью спец. электронных устройств внедренных в помещение, в котором ведется обработка ПДн | 0  (маловероятно) | 0,25 | | низкая | неактуальная | Жалюзи на окна | Пропускной режим на объекте, контроль доступа в помещения ИС |
| * 1. **Угрозы утечки информации по каналам ПЭМИН – в соответствии с п. 7.1.3 «Общая модель угроз верхнего уровня Администрации Чамзинского муниципального района Республики Мордовия данные каналы утечки информации не рассматриваются.** | | | | | | | |
| 1. **Угрозы несанкционированного доступа к информации** | | | | | | | |
| * 1. **Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИС** | | | | | | | |
| Кража ПЭВМ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Охранная сигнализация | Пропускной режим, физическая охрана, видеонаблюдение в пределах КЗ |
| Кража носителей информации | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Охранная сигнализация | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| Кража ключей и атрибутов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Модификация и уничтожение информации. | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим.  Видеонаблюдение в пределах КЗ |
| Вывод из строя узлов ПЭВМ, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Выполнение организационных мер,  инструкции персоналу,  пропускной режим |
| Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ | 5  (средняя) | 0,5  (средняя) | | высокая | **актуальная** | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| Несанкционированное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Выполнение организационных мер, инструкции персоналу, пропускной режим |
| **2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)** | | | | | | | |
| Угроза внедрения вредоносных программ | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| Недекларированные возможности системного ПО и ПО для обработки ПДн | 0  (маловероятно) | 0,25  (низкая) | | Низкая | неактуальная |  | Инструкции администратору |
| Установка ПО, не связанного с исполнением служебных обязанностей, в т.ч. для выполнения НСД | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС Windows | Инструкции персоналу и администратору, установка только разрешенного ПО |
| Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИС | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Внедрение аппаратных закладок сотрудниками организации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору |
| Модификация BIOS, перехват управления загрузкой операционной системы | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Перехват паролей, идентификаторов при входе в систему | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, контроль доступа в помещения ИСПДн |
| **2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.** | | | | | | | |
| Утрата ключей доступа | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции персоналу и администратору |
| Непреднамеренное внедрение вредоносных программ с внешних носителей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору, Учет носителей информации |
| Непреднамеренная модификация (уничтожение) информации сотрудниками | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование баз данных по расписанию | Инструкции персоналу и администратору |
| Непреднамеренное отключение средств защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС и СЗИ НСД | Инструкции персоналу и администратору |
| Выход из строя аппаратно-программных средств | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств | Инструкции администратору |
| Сбой системы электроснабжения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Стихийные бедствия | 0  (маловероятно) | 0,5  (средняя) | | низкая | неактуальная | Резервирование аппаратно-программных средств | Инструкции персоналу и администратору |
| **2.4 Угрозы преднамеренных действий внутренних нарушителей** | | | | | | | |
| Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИСПДн |
| Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Организационные мероприятия, инструкции персоналу |
| **2.5 Угрозы несанкционированного доступа по каналам связи** | | | | | | | |
| Анализ сетевого трафика | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ, использование VPN | Инструкции персоналу и администратору |
| Перехват в пределах контролируемой зоны внешними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Перехват в пределах контролируемой зоны внутренними нарушителями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору,  контроль доступа в помещения ИС |
| Сканирование сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угроза выявления паролей | 2  (низкая) | 0,35  (средняя) | | средняя | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы навязывание ложного маршрута сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Угрозы подмены доверенного объекта | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СКЗИ | Инструкции персоналу и администратору |
| Внедрение ложного объекта сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы типа «Отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки МЭ | Инструкции персоналу и администратору |
| Угрозы удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции персоналу и администратору |
| Угрозы внедрения по сети вредоносных программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции персоналу и администратору |
| **2.6 Угрозы перехвата при передаче по проводным (кабельным) линиям связи** | | | | | | | |
| Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Расположение узлов связи в недоступных для нарушителя местах.  Шифрование сетевого трафика | Физическая охрана, инструкции персоналу, расположение ИС в одном (смежных) помещении |
| Анализ сетевого трафика в пределах контролируемой зоны внутренними нарушителями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |
| **3. Угрозы использования штатных средств ИС с целью совершения НСД к информации** | | | | | | | |
| Угроза некорректного использования функционала программного обеспечения | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного изменения аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкция администратор |
| Угроза несанкционированного использования привилегированных функций BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Смена пароля в соответствии с инструкцией администратора |
| Доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Установка только разрешенного ПО |
| **4. Угрозы нарушения доступности информации** | | | | | | | |
| Угроза длительного удержания вычислительных ресурсов пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отказа в обслуживании системой хранения данных суперкомпьютера | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перегрузки грид-системы вычислительными заданиями | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза повреждения системного реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Резервирование ОС, настройка прав доступа |
| Угроза приведения системы в состояние «отказ в обслуживании» | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Использование отказоустойчивого ПО |
| Угроза утраты вычислительных ресурсов | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция админисратора |
| Угроза вывода из строя/выхода из строя отдельных ТС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервирование аппаратно-программных средств |  |
| Угроза вывода из строя незарезервированных ТС/программных средств/каналов связи | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервирование аппаратно-программных средств |  |
| Угроза отсутствия актуальных резервных копий информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Резервное копирование |
| Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Шифрование сетевого трафика |  |
| Угроза переполнения канала связи вследствие множества параллельных попыток авторизации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза нехватки ресурсов ИС для выполнения штатных задач в результате обработки множества параллельных задач, выполняемых одной учетной записью | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Своевременная замена компонентов АРМ |
| Угроза вывода из строя ИС при подаче на интерфейсы информационного обмена «неожидаемой» информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| **5. Угрозы нарушения целостности информации** | | | | | | | |
| Угроза нарушения целостности данных кеша | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза подмены содержимого сетевых ресурсов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Шифрование сетевого трафика |  |
| Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя обработки специальным образом изменённых файлов | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля целостности обрабатываемой в ИС информации, применяемого программного обеспечения, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия целостных резервных копий информации, программного обеспечения, СЗИ в случае реализации угроз информационной безопасности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Резервное копирование |  |
| Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза доступа в ИС информации от не аутентифицированных серверов/пользователей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройки СЗИ НСД | Инструкции пользователя администратора |
| Угроза отсутствия контроля за данными, передаваемыми из ИС | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Отсутствие резервного копирования информации, передаваемой из ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование баз данных по расписанию |  |
| Угроза передачи из ИС недопустимой информации | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Антивирусное ПО, Настройка МЭ |  |
| Угроза ввода/передачи недостоверных/ошибочных данных | 5  (средняя) | 0,5  (средняя) | | низкая | неактуальная |  | Инструкция пользователя |
| Угроза подмены используемых ИС файлов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя, пропускной режим |
| Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО пользователя и администратора |
| Угроза модификации/стирания/удаления данных системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Отсутствие регламента/графика проведения контроля целостности применяемых программных средств, в том числе СЗИ | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| **6. Угрозы, не являющиеся атаками** | | | | | | | |
| Угроза исчерпания вычислительных ресурсов хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неверного определения формата входных данных, поступающих в хранилище больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза неконтролируемого уничтожения информации хранилищем больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  |  |
| **7. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации** | | | | | | | |
| Угроза аппаратного сброса пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системного блока,  Контроль интерфейсов ввода-вывода, инструкция администратора |
| Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Настройка СЗИ НСД |  |
| Угроза обхода некорректно настроенных механизмов аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, выполнение парольной политики |
| Угроза программного сброса пароля BIOS | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС | Перечень разрешенного к установке ПО, ограничение на установку ПО |
| Угроза «кражи» учётной записи доступа к сетевым сервисам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза получения доступа к ИС, компонентам ИС, информации, обрабатываемой ИС без прохождения процедуры идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС, контроль интерфейсов ввода-вывода |
| Угроза получения доступа к ИС вследствие ошибок подсистемы идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза получения несанкционированного доступа сторонними лицами, устройствами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте |
| Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угрозы авторизации с использованием устаревших, но не отключённых учетных записей | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза использования «слабых» методов идентификации и аутентификации пользователей, в том числе при использовании удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза применения только программных методов двухфакторной аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования долговременных паролей для подключения к ИС посредством удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза передачи аутентифицирующей информации по открытым каналам связи без использования криптографических СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СКЗИ | Инструкции пользователя и администратора |
| Угроза доступа к ИС неаутентифицированных устройств и пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза повторного использования идентификаторов в течение как минимум 1 года | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза использования идентификаторов, неиспользуемых более 45 дней | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя, выполнение парольной политики |
| Угроза раскрытия используемых идентификаторов пользователя в публичном доступе | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие управления идентификаторами внешних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования «слабых»/предсказуемых паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД |  |
| Угроза использования пользователями идентичных идентификаторов в разных информационных системах | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Угроза отсутствия регламента работы с персональными идентификаторами | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя |
| Отсутствие в централизованной системе идентификации и аутентификации атрибутов, позволяющих однозначно определить внешних и внутренних пользователей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза бесконтрольного доступа пользователей к процессу загрузки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция пользователя и адмиистратора |
| Угроза подмены/модификации базовой системы ввода-вывода, программного обеспечения телекоммуникационного оборудования | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Контроль доступа в помещения ИС |
| **8. Угрозы НСД к информации в результате слабости процедур разграничения ролей и полномочий, правил управления доступом** | | | | | | | |
| Угроза воздействия на программы с высокими привилегиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Использование СЗИ |  |
| Угроза доступа к защищаемым файлам с использованием обходного пути | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза доступа к локальным файлам сервера при помощи URL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза загрузки нештатной ОС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Контроль доступа в помещения ИС, контроль портов ввода вывода, инструкции пользователя и администратора |
| Угроза изменения системных и глобальных переменных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза использования альтернативных путей доступа к ресурсам | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза использования механизмов авторизации для повышения привилегий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора |
| Угроза нарушения изоляции среды исполнения BIOS |  |  | |  |  | Настройка СЗИ НСД |  |
| Угроза невозможности управления правами пользователей BIOS |  |  | |  |  | Настройка СЗИ НСД | Инструкция администратора |
| Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки ОС | Инструкции пользователя и администратора |
| Угроза неправомерного ознакомления с защищаемой информацией | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Перечень лиц, допущенных к обработке |
| Угроза несанкционированного доступа к аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза несанкционированного доступа к системе по беспроводным каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного копирования защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза несанкционированного редактирования реестра | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Ограничение на установку ПО |
| Угроза несанкционированного создания учётной записи пользователя | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора и пользователя |
| Угроза несанкционированного управления буфером | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления синхронизацией и состоянием | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированного управления указателями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза передачи запрещённых команд на оборудование с числовым программным управлением | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза повышения привилегий |  |  | |  |  | Антивирусное ПО | Инструкция пользователя |
| Угроза подбора пароля BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | неакутальная |  | Инструкция администратора |
| Угроза подделки записей журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора, установка только разрешенного ПО |
| Угроза эксплуатации цифровой подписи программного кода | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО |  |
| Угроза доступа к информации и командам, хранящимся в BIOS, с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя и администратора |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора |
| Угроза получения доступа к данным в обход механизмов разграничения доступа, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения разными пользователей, лицами, обеспечивающими функционирование, доступа к данным и полномочиям, не предназначенными для данных лиц в связи с их должностными обязанностями | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция пользователя и администратора, контроль доступа в помещения ИС |
| Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция пользователя и администратора |
| Отсутствие ограничения на количество неудачных попыток входа в информационную систему | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора |
| Угроза использования (подключения) к открытому(незаблокированному) сеансу пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка ОС | Инструкция пользователя |
| Угроза использования ресурсов ИС до прохождения процедур идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угрозы несанкционированного подключения к ИС с использованием санкционированной сессии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подбора идентификационных данных для удаленного доступа к ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция пользователя |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, в том числе мобильных устройств без прохождения процедуры идентификации и авторизации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения доступа к ИС с использованием технологий беспроводного доступа, с неконтролируемых устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза несанкционированной автоматической передачи конфиденциальной информации на запросы сторонних информационных систем | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза получения несанкционированного доступа к средствам управления персональными идентификаторов/учетными записями, в том числе с повышенными правами доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза получения несанкционированного доступа к средствам управления средствами идентификации и аутентификации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора, контроль доступа в помещения ИС |
| Угроза бесконтрольного доступа к информации неопределенным кругом лиц | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза получения доступа к данным, не предназначенным для пользователя | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ НСД |  |
| Угроза удаленного управления и использования периферийных устройств для получения информации или выполнения иных деструктивных целей | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД) |  |
| Угроза использования технологий мобильного кода для совершения попыток несанкционированного доступа к ИС при использовании в ИС мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования встроенных в информационную систему недекларированных возможностей, скрытых каналов передачи информации в обход реализованных мер защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие отказоустойчивых централизованных средств управления учетными записями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия необходимых методов управления доступом для разграничения прав доступа в соответствии с технологией обработки и угрозами безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза передачи информации без соблюдения атрибутов(меток) безопасности, связанных с передаваемой информацией | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие динамического анализа и управления информационными потоками в зависимости от состояния ИС, условий ее функционирования, изменений в технологии обработки, передаваемых данных | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза обхода правил управления информационными потоками за счет манипуляций с передаваемыми данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза возложения функционально различных должностных обязанностей/ролей на одно должностное лицо | 2  (низкая) | 0,35  (средняя) | | 0  (маловероятно) | 0,25  (низкая) |  | Выполнение организационных мер |
| Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗ НСД | Инструкция администратора |
| Отсутствие информирования пользователя о применении СЗИ и необходимости соблюдения установленных оператором правил и ограничений на работу с информацией, о предыдущем успешном доступе к ИС, о количестве успешных/неуспешных попыток доступа, об изменении сведений об учетной записи пользователя, о превышении числа параллельных сеансов доступа | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройки СЗИ | Инструкция пользователя |
| Отсутствие информирования администратора о превышении числа параллельных сеансов доступа пользователями | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования одних и тех же учетных записей для параллельного доступа к ИС (с 2 и более) различных устройств | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза использования незавершенных сеансов пользователей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка ОС | Инструкции пользователя |
| Угроза наличия удаленного доступа от имени привилегированных пользователей для администрирования ИС, системы защиты, в том числе с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции пользователя и администратора |
| Отсутствие автоматизированного мониторинга и контроля удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза использования уязвимых/незащищенных технологий удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза взаимодействия с иными информационными системами, не обеспеченными системой защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Отсутствие механизмов автоматизированного контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие механизмов автоматизированного реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие контроля за используемыми интерфейсами ввода/вывода | 2  (средняя) | 0,35  (средняя) | | средняя | актуальная |  | Контроль интерфейсов ввода-вывода, инструкции администратора и пользователя |
| **9. Угрозы ошибок/внесения уязвимостей при проектировании, внедрении ИС/системы защиты ИС** | | | | | | | |
| Угроза передачи данных по скрытым каналам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ | Инструкция администратора |
| Угроза включения в проект не испытанных достоверно компонентов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза внедрения системной избыточности | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза ошибок при моделировании угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| Угроза внедрения системы защиты, не обеспечивающей нивелирования актуальных угроз и нарушителей информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Ежегодная доработка модели угроз, повышение квалификации специалистов по защите информации |
| **10. Угрозы ошибочных/деструктивных действий лиц** | | | | | | | |
| Угроза подмены действия пользователя путём обмана | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза «фишинга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Реализация угроз с использованием возможности по непосредственному доступу к техническим и части программных средств ИС, СЗИ и СКЗИ, в соответствии с установленными для них административными полномочиями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС |
| Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/частичному отключению ИС/модулей/компонентов/сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации) | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | СЗИ НСД | Инструкции администратора и пользователя, контроль доступа в помещения ИС, опломбирование ПЭВМ |
| Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкции пользователя |
| Переконфигурирование СЗИ и СКЗИ для реализации угроз ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции СКЗИ пользователя и администратора |
| Осуществление угроз с использованием локальных линий связи, систем электропитания и заземления | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение в пределах КЗ, инструкция пользователя |
| Хищение ключей шифрования, идентификаторов и известных паролей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя, контроль доступа в помещения ИС |
| Внесение программно-аппаратных закладок в программно - аппаратные средства ИС, обеспечивающих съем информации, используя непосредственное подключение к техническим средствам обработки информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Создание методов и средств реализации атак, а также самостоятельное проведение атаки | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя |
| Ошибки при конфигурировании и обслуживании модулей/компонентов ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Создание ситуаций, препятствующих функционированию сети (остановка, сбой серверов; уничтожение и/или модификация программного обеспечения; создание множественных, ложных информационных сообщений) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Несанкционированный съем информации, блокирование работы отдельных пользователей, перестройка планов маршрутизации и политик доступа сети. | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Непреднамеренное разглашение ПДн лицам, не имеющим права доступа к ним | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Нарушение правил хранения ключевой информации | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Передача защищаемой информации по открытым каналам связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика | Инструкции пользователя и администратора |
| Несанкционированная модификация/уничтожение информации легитимным пользователем | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя |
| Копирование информации на незарегистрированный носитель информации, в том числе печать | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Выполнение организационных мер, инструкции пользователя и администратора |
| Несанкционированное отключение средств защиты | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** | Настройки ОС и СЗИ НСД | Инструкции пользователя и администратора |
| Угрозы вербовки (социальной инженерии) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| **11. Угрозы нарушения конфиденциальности** | | | | | | | |
| Угроза исследования механизмов работы программы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя и администратора |
| Угроза исследования приложения через отчёты об ошибках | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Контроль доступа к журналам, инструкция администратора |
| Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза обнаружения хостов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения типов объектов защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза определения топологии вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения предварительной информации об объекте защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения сведений о владельце беспроводного устройства | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Сканирование сети для изучения логики работы ИС, выявления протоколов, портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Анализ сетевого трафика для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем сведений о структуре, конфигурации и настройках ИС и ее системы защиты | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Угроза получения нарушителем идентификационных данных легальных пользователей ИС | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим, контроль доступа в помещения ИС, инструкции пользователя и администратора |
| Разглашение сведений конфиденциального характера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Организационные мероприятия, инструкция пользователя |
| **12. Угрозы программно-математических воздействий** | | | | | | | |
| Угроза автоматического распространения вредоносного кода в грид-системе | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза внедрения кода или данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза восстановления аутентификационной информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкция администратора и пользователя |
| Угроза деструктивного изменения конфигурации/среды окружения программ | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| Угроза избыточного выделения оперативной памяти | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкция пользователя |
| Угроза искажения XML-схемы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза искажения вводимой и выводимой на периферийные устройства информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабостей кодирования входных данных | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная | Использование СКЗИ |  |
| Угроза межсайтового скриптинга | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза межсайтовой подделки запроса | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя |
| Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза перехвата вводимой и выводимой на периферийные устройства информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ | Выполнение организационных мер, контроль периметра |
| Угроза подмены резервной копии программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкция администратора, контроль доступа в помещения ИС |
| Угроза заражения компьютера при посещении неблагонадёжных сайтов | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО |  |
| Угроза неправомерного шифрования информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Установка только разрешенного ПО, инструкция пользователя |
| Угроза скрытного включения вычислительного устройства в состав бот-сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Установка только разрешенного ПО, инструкция пользователя |
| Угроза распространения «почтовых червей» | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Внедрение программных закладок | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза внедрения в ИС вредоносного программного обеспечения с устройств, подключаемых с использованием технологий беспроводного доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Антивирусное ПО | Инструкции пользователя и администратора |
| Применение специально созданных программных продуктов для НСД | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Отсутствие централизованной системы управления средствами антивирусной защиты | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкция администратора |
| **13. Угрозы, связанные с использованием технологий виртуализации – соответствии с п.6.13 Общей модели угроз Администрации Чамзинского муниципального района данные угрозы не рассматриваются.** | | | | | | | |
| **14. Угрозы, связанные с нарушением правил эксплуатации машинных носителей** | | | | | | | |
| Угроза несанкционированного восстановления удалённой защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Установка только разрешенного ПО, инструкции пользователя и администратора |
| Угроза несанкционированного удаления защищаемой информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза утраты носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, инструкции пользователя и администратора |
| Угроза форматирования носителей информации | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Резервное копирование | Инструкции пользователя и администратора |
| Повреждение носителя информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Резервное копирование |  |
| Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные) | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, контроль доступа в помещение |
| Угроза подключения к ИС неучтенных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза подключения к ИС неперсонифицированных машинных носителей | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации |
| Угроза несанкционированного копирования информации на машинные носители | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза несанкционированной модификации/удаления информации на машинных носителях | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза хищения машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза подмены машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, пропускной режим |
| Угроза встраивания программно-аппаратных закладок в машинные носители | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД | Инструкция администратора пользователя, учет носителей информации |
| Угроза несанкционированного доступа к информации, хранящейся на машинном носителе | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Учет носителей информации, хранение в сейфе |
| Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора |
| Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкции пользователя и администратора, контроль интерфейсов ввода-вывода |
| Угроза передачи информации/фрагментов информации между пользователями, сторонними организациями при неполном уничтожении/стирании информации с машинных носителей | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкции пользователя и администратора |
| Угроза несанкционированного использования машинных носителей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе |
| Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны | 5  (высокая) | 0,5  (средняя) | | средняя | **актуальная** |  | Учет носителей информации, хранение в сейфе, видеонаблюдение в пределах КЗ |
| **15 Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования** | | | | | | | |
| Угроза внедрения вредоносного кода в BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Пароль на BIOS | Инструкция администратора |
| Угроза изменения компонентов системы | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Опломбирование системных блоков, инструкция администратора |
| Угроза установки на мобильные устройства вредоносных/уязвимых программных продуктов | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | средняя | | **актуальная** |  | Инструкции администратора и пользователя |
| Установка программного обеспечения, содержащего известные уязвимости | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция пользователя и администратора |
| Установка нелицензионного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции администратора и пользователя |
| Угроза ошибочного запуска/установки программного обеспечения | 5  (средняя) | 0,5  (средняя) | | средняя | **актуальная** |  | Инструкции администратора и пользователя |
| Угроза неправильной установки программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза автоматического запуска вредоносного/шпионского/неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СЗИ | Инструкция администратора |
| Угроза удаленного запуска/установки вредоносного/шпионского/неразрешенного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД | Инструкции администратора и пользователя |
| Угроза несанкционированного запуска программного обеспечения в нерабочее время | 2  (низкая) | 0,25  (низкая) | | низкая | неактуальная |  | Инструкция пользователя |
| **16. Угрозы физического доступа к компонентам ИС** | | | | | | | |
| Угроза преодоления физической защиты | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Физическая охрана |
| Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте, контроль доступа в помещения ИС, видеонаблюдение в пределах КЗ |
| Угроза несанкционированного доступа к системам криптографической защиты информации (СКЗИ) | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза нарушения функционирования НЖМД и других систем хранения данных | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза доступа к системам обеспечения, их повреждение | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Физическая охрана, контроль доступа в помещения |
| Угроза нарушения функционирования кабельных линий связи, ТС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, контроль доступа в помещения ИС |
| Угроза несанкционированного доступа в контролируемую зону | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Пропускной режим на объекте, видеонаблюдение пределах КЗ |
| Отсутствие средств автоматизированного контроля доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Физическая охрана, пропускной режим на объекте |
| **17. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении** | | | | | | | |
| Угроза анализа криптографических алгоритмов и их реализации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза восстановления предыдущей уязвимой версии BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза деструктивного использования декларированного функционала BIOS | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Пароль BIOS |
| Угроза использования поддельных цифровых подписей BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза использования слабых криптографических алгоритмов BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ НСД |  |
| Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза отключения контрольных датчиков | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Антивирусное ПО | Инструкции пользователя и администратора |
| Угроза распространения несанкционированно повышенных прав на всю грид-систему | Угроза является неактуальной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза сбоя процесса обновления BIOS | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная |  | Инструкция администратора |
| Угроза установки уязвимых версий обновления программного обеспечения BIOS | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза перехвата исключения/сигнала из привилегированного блока функций | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза наличия механизмов разработчика | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза «спама» веб-сервера | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| **18. Угрозы, связанные с использованием сетевых технологий** | | | | | | | |
| Угроза деавторизации санкционированного клиента беспроводной сети | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза заражения DNS-кеша | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка МЭ |  |
| Угроза использования слабостей протоколов сетевого/локального обмена данными | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Угроза неправомерных действий в каналах связи | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СЗИ НСД |  |
| Угроза подключения к беспроводной сети в обход процедуры идентификации/аутентификации | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены беспроводного клиента или точки доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены доверенного пользователя | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза подмены субъекта сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза «фарминга» | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкции пользователя и администратора |
| Угроза агрегирования данных, передаваемых в грид-системе | Угроза является неактульной, т.к. данная технология не используется в ИС | | | | | | |
| Угроза удаленного запуска приложений | 2  (низкая) | 0,35  (средняя) | | низкая | неактуальная | Настройка СЗИ НСД | Инструкции пользователя и администратора |
| Угроза навязывания ложных маршрутов | 0  (маловероятно) | 0,25  (низкая)) | | средняя | неактуальная | Настройки СКЗИ | Инструкции пользователя и администратора |
| Угроза внедрения ложных объектов сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ | Инструкции пользователя и администратора |
| Угроза проведения атак/попыток несанкционированного доступа на ИС с использованием протоколов сетевого доступа | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия механизмов реагирования (блокирования) атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки МЭ |  |
| Угроза отсутствия системы анализа сетевого трафика между сегментами ИС на наличие атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза использования неактуальных версий сигнатур обнаружения атак | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза отсутствия централизованной системы управления средствами защиты от атак/вторжений | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ, Настройки СЗИ |  |
| Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ НСД |  |
| Угроза бесконтрольного использования технологий беспроводного доступа, в том числе с мобильных устройств | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза подмены устройств, подключаемых к ИС с использованием технологии удаленного доступа | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| Угроза использования неконтролируемых сетевых протоколов для модификации/перехвата управления ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза перехвата, искажения, модификации, подмены, перенаправления трафика между разными категориями пользователей и СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ | Инструкции администратора и пользователя |
| Угроза подмены сетевых адресов, определяемых по сетевым именам | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия проверки подлинности сетевых соединений | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройки СКЗИ |  |
| Отсутствие подтверждения факта отправки/получения информации конкретными пользователями | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки СКЗИ |  |
| Угроза получения несанкционированного доступа при двунаправленной передаче информации между сегментами, информационными системами | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Отсутствие контроля соединений между СВТ ИС | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза несанкционированного доступа к средствам управления информационными потоками | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  |  |
| Угроза отсутствия/неиспользования средств разделения информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской  информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Шифрование сетевого трафика |  |
| Отсутствие средств анализа сетевого трафика на наличие вредоносного программного обеспечения | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа к ИС с использованием беспроводного доступа из-за границ контролируемой зоны | 0  (маловероятно) | 0,25  (низкая) | | низкая | неактуальная |  |  |
| **19. Угрозы инженерной инфраструктуры** | | | | | | | |
| Угрозы сбоев в сети электропитания | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Использование  ИБП | Резервное копирование |
| Угроза выхода из строя ТС в результате нарушения климатических параметров работы | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы нарушения схем электропитания | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| Угрозы связанные с отсутствием заземления/неправильным заземлением | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Резервирование аппаратно-программных средств |  |
| **20. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности** | | | | | | | |
| Угроза отсутствия системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ |  |
| Угроза автоматического удаления/затирания событий информационной безопасности новыми события | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза переполнения журналов информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованного подсистемы централизованного сбора событий информационной безопасности от различных программных и аппаратных продуктов, СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза неправильного отнесения событий, к событиям информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия централизованной системы анализа журналов информационной безопасности от различных программных и аппаратных продуктов, средств СЗИ | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза модификации/удаления журнала информационной безопасности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** | Настройка СЗИ | Инструкция администратора |
| Угроза задержек при получении журналов информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза ошибок ведения журнала регистрации событий информационной безопасности, в том числе связанных с неправильными настройками времени | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отсутствия необходимых сведений в журналах информационной безопасности для проведения проверки/расследования/анализа событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза отключения/отказа системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Угроза несанкционированного изменения правил ведения журнала регистрации событий | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| Отсутствие оповещений (предупреждений) администратора о сбоях, критических событиях в работе системы регистрации событий информационной безопасности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройка СЗИ | Инструкция администратора |
| **21. Угрозы, связанные с контролем защищенности ИС** | | | | | | | |
| Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Контроль доступа в помещения ИС, установка только разрешенного ПО |
| Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей | 2  (низкая) | 0,35  (средняя) | | средняя | **актуальная** |  | Инструкция администратора |
| Угроза отсутствия регулярного контроля за защищенностью ИС, в том числе СЗИ с учетом новых угроз безопасности информации | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Угроза отсутствия анализа изменения настроек ИС, компонентов ИС, в том числе СЗИ на предмет появления уязвимостей\* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| Отсутствие журнала анализа защищенности | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная |  | Инструкция администратора |
| **22. Угрозы, связанные с перехватом защищаемой информации при ее передаче по каналам связи** | | | | | | | |
| Угроза перехвата данных, передаваемых по вычислительной сети | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза доступа/перехвата/изменения HTTP cookies | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных \* | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных, передаваемых по сетям внешнего и международного информационного обмена | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |
| Угроза перехвата данных с сетевых портов | 0  (маловероятно) | 0,25  (низкая) | | средняя | неактуальная | Настройки МЭ |  |

1. **Выводы и рекомендации**
   1. Для ИС «Администрация Чамзинского муниципального района Республики Мордовия» актуальными угрозами безопасности ПДн являются:
      1. Угрозы утечки видовой информации:

* Просмотр информации на дисплее сотрудниками, не допущенными к обработке ПДн.
  + 1. Угрозы уничтожения, хищения аппаратных средств ИС и носителей информации путем физического доступа к элементам ИСПДн:
* Кража ПЭВМ;
* Кража носителей информации;
* Модификация и уничтожение информации;
* Вывод из строя узлов ПЭВМ, каналов связи;
* Несанкционированный доступ к информации при техническом обслуживании (ремонте) узлов ПЭВМ;
* Несанкционированное отключение средств защиты.
  + 1. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):
* Угроза внедрения вредоносных программ;
* Установка ПО, не связанного с исполнением служебных обязанностей, в том числе для выполнения НСД;
* Перехват паролей, идентификаторов при входе в систему.
  + 1. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:
* Утрата ключей доступа;
* Непреднамеренное внедрение вредоносных программ с внешних носителей;
* Непреднамеренная модификация (уничтожение) информации сотрудниками;
* Выход из строя аппаратно-программных средств;
* Стихийные бедствия;
  + 1. Угрозы преднамеренных действий внутренних нарушителей:
* Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;
* Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
  + 1. Угрозы несанкционированного доступа по каналам связи:
* Угрозы внедрения по сети вредоносных программ.
  + 1. Угрозы перехвата при передаче по проводным (кабельным) линиям связи:
* Анализ сетевого трафика в пределах контролируемой зоны внешними нарушителями
  + 1. Угрозы использования штатных средств ИС с целью совершения НСД к информации:
* Угроза несанкционированного изменения аутентификационной информации.
  + 1. Угрозы нарушения доступности информации
* Угроза повреждения системного реестра.
* Угроза вывода из строя/выхода из строя отдельных ТС.
* Угроза потери информации в процессе ее обработки технически и(или) программными средствами и при передаче по каналам связи.
  + 1. Угрозы нарушения целостности информации:
* Угроза отсутствия контроля за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие средств централизованного управления за поступающими в информационную систему данными, в том числе незапрашиваемыми.
* Отсутствие автоматизированных фильтров, осуществляющих обработку поступающей в ИС информации.
* Угроза отсутствия контроля за данными, передаваемыми из ИС.
* Отсутствие резервного копирования информации, передаваемой из ИС.
* Угроза передачи из ИС недопустимой информации.
* Угроза подмены используемых ИС файлов.
* Угроза модификации/удаления файлов журналов системного, прикладного ПО, средств защиты.
* Угроза установки/запуска модифицированного программного обеспечения и (или) модифицированных обновлений программного обеспечения.
  + 1. Угрозы, не являющиеся атаками:
* Угроза выхода из строя/отказа отдельных ТС, программных средств, каналов связи.
  + 1. Угрозы НСД, создающие предпосылки для реализации НСД в результате нарушения процедуры авторизации и аутентификации:
* Угроза аппаратного сброса пароля BIOS.
* Угроза обхода некорректно настроенных механизмов аутентификации.
* Угроза программного сброса пароля BIOS.
* Угроза получения несанкционированного доступа сторонними лицами, устройствами.
* Угроза отсутствия/слабости процедур аутентификации при доступе пользователей/устройств к ресурсам ИС.
* Угрозы авторизации с использованием устаревших, но не отключённых учетных записей.
* Угроза доступа к ИС неаутентифицированных устройств и пользователей.
* Угроза повторного использования идентификаторов в течение как минимум 1 года.
* Угроза раскрытия используемых идентификаторов пользователя в публичном доступе.
* Угроза использования «слабых» /предсказуемых паролей.
* Отсутствие отказоустойчивой централизованной системы идентификации и аутентификации.
* Угроза использования пользователями идентичных идентификаторов в разных информационных системах.
* Угроза отсутствия регламента работы с персональными идентификаторами.
* Угроза доступа к защищаемым файлам с использованием обходного пути.
* Угроза загрузки нештатной ОС.
* Угроза использования альтернативных путей доступа к ресурсам.
* Угроза несанкционированного доступа к аутентификационной информации.
* Угроза несанкционированного копирования защищаемой информации.
* Угроза несанкционированного редактирования реестра.
* Угроза несанкционированного создания учётной записи пользователя.
* Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
* Угроза удаления аутентификационной информации.
* Угроза предоставления прав доступа, не необходимых для исполнения должностных обязанностей и функционирования ИС, для совершения деструктивных действий.
* Отсутствие ограничения на количество неудачных попыток входа в информационную систему.
* Угроза перехвата идентифицирующих и аутентифицирующих данных в процессе идентификации и аутентификации пользователей.
* Угроза бесконтрольного доступа к информации неопределенным кругом лиц.
* Отсутствие автоматического блокирования учетных записей по истечении их срока действия, в результате исчерпания попыток доступа к ИС, выявления попыток НСД.
* Угроза предоставления расширенных прав и привилегий пользователям, в том числе внешним.
* Угроза использования незавершенных сеансов пользователей.
* Отсутствие контроля за используемыми интерфейсами ввода/вывода.
  + 1. Угрозы ошибочных/деструктивных действий лиц:
* Внесение изменений в конфигурацию программных средств и ТС, приводящими к отключению/ частичному отключению ИС/ модулей/ компонентов/ сегментов ИС, СЗИ (в случае сговора с внешними нарушителями безопасности информации).
* Создание неконтролируемых точек доступа (лазейки) в систему, для удаленного доступа к ИС.
* Хищение ключей шифрования, идентификаторов и известных паролей.
* Несанкционированная модификация/уничтожение информации легитимным пользователем.
* Копирование информации на незарегистрированный носитель информации, в том числе печать.
* Несанкционированное отключение средств защиты.
  + 1. Угрозы нарушения конфиденциальности:
* Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
* Угроза получения нарушителем конфиденциальных сведений, обрабатываемых в ИС.
* Угроза получения нарушителем идентификационных данных легальных пользователей ИС.
  + 1. Угрозы программно-математических воздействий:
* Угроза внедрения кода или данных.
* Угроза восстановления аутентификационной информации.
* Угроза деструктивного изменения конфигурации/среды окружения программ.
* Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
* Угроза перехвата вводимой и выводимой на периферийные устройства информации.
* Угроза заражения компьютера при посещении неблагонадёжных сайтов.
* Угроза неправомерного шифрования информации.
* Угроза распространения «почтовых червей».
* Внедрение программных закладок.
* Применение специально созданных программных продуктов для НСД.
* Угроза внедрения через легитимные схемы информационного обмена между информационными системами вредоносного программного обеспечения.
* Отсутствие централизованной системы управления средствами антивирусной защиты.
  + 1. Угрозы, связанные с нарушением правил эксплуатации машинных носителей:
* Угроза несанкционированного восстановления удалённой защищаемой информации.
* Угроза несанкционированного удаления защищаемой информации.
* Угроза утраты носителей информации.
* Угроза форматирования носителей информации.
* Повреждение носителя информации.
* Угроза подключения к ИС неучтенных машинных носителей.
* Угроза подключения к ИС неперсонифицированных машинных носителей.
* Угроза несанкционированного копирования информации на машинные носители.
* Угроза несанкционированной модификации/удаления информации на машинных носителях.
* Угроза хищения машинных носителей.
* Угроза подмены машинных носителей.
* Угроза использования машинных носителей для хранения информации разных уровней конфиденциальности и целей обработки.
* Угроза использования неконтролируемых портом СВТ для вывода информации на сторонние машинные носители.
* Угроза несанкционированного использования машинных носителей.
* Угроза несанкционированного выноса машинных носителей за пределы контролируемой зоны.
  + 1. Угрозы, связанные с нарушением процедур установки/обновления программного обеспечения и оборудования:
* Угроза внедрения вредоносного кода в BIOS.
* Угроза изменения компонентов системы.
* Угроза запуска/ установки вредоносного/ шпионского/ неразрешенного программного обеспечения и(или) обновлений программного обеспечения.
* Угроза ошибочного запуска/установки программного обеспечения.
* Угроза автоматического запуска вредоносного/ шпионского/ неразрешенного программного обеспечения при запуске ОС и(или) обновлений программного обеспечения.
* Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
* Угроза нарушения функционирования НЖМД и других систем хранения данных.
* Отсутствие средств автоматизированного контроля доступа.
  + 1. Угрозы эксплуатации уязвимостей в СПО, ППО, СЗИ, СКЗИ, аппаратных компонентах ИСПДн, микропрограммном обеспечении:
* Угроза восстановления предыдущей уязвимой версии BIOS.
* Угроза деструктивного использования декларированного функционала BIOS.
* Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
  + 1. Угрозы, связанные с использованием сетевых технологий:
* Угроза отсутствия системы анализа сетевого трафика при обмене данными между информационными системами на наличие атак/вторжений.
* Угроза использования слабостей/уязвимостей защиты протоколов удаленного доступа.
* Угроза отсутствия проверки подлинности сетевых соединений.
  + 1. Угрозы инженерной инфраструктуры:
* Угрозы сбоев в сети электропитания.
  + 1. Угрозы, связанные с отсутствием системы регистрации событий информационной безопасности:
* Угроза автоматического удаления/затирания событий информационной безопасности новыми события.
* Угроза переполнения журналов информационной безопасности.
* Угроза неправильного отнесения событий, к событиям информационной безопасности.
* Угроза модификации/удаления журнала информационной безопасности
  + 1. Угрозы, связанные с контролем защищенности ИС:
* Угроза отсутствия контроля за уязвимостями ИС, компонентов ИС, наличием неразрешенного программного обеспечения.
* Угроза использования неактуальных версий баз данных уязвимостей средств анализа защищенности.
* Угроза установки программного обеспечения/обновлений без проведения анализа уязвимостей.
  1. Для предотвращения реализации выявленных для ИС актуальных угроз в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства криптографической защиты;
* реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
* методы и средства аутентификации пользователей, паролей и логинов доступа;
* мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке информации;
* регулярный инструктаж пользователей о мерах предотвращения вирусного заражения;
* организация постоянного контроля за выполнением пользователями инструкций по обеспечению защиты информации, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей;
* периодическое резервное копирование обрабатываемых данных на учтенные носители информации;
* подписание пользователями документа о неразглашении информации.
  1. Актуальные угрозы безопасности, представленные в данной Модели угроз, подлежат проработке на этапах выбора мер защиты информации.

|  |  |
| --- | --- |
| Глава Чамзинского муниципального района | В.Г. Цыбаков |
| «\_\_\_» **\_\_\_\_\_\_\_\_\_\_\_** 2019 г. |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Главный редактор:**

**начальник отдела администрации**

**Чамзинского муниципального района**

**по обеспечению взаимодействия с представительным органом Н.В. Козырева**

**адрес: р.п. Чамзинка, ул. Победы, д. 1**

**эл.почта: inform113@mail.ru**

**тел: 2-12-43, 2-12-00 факс: 2-12-00**