**АДМИНИСТРАЦИЯ**

**УСТЬ-БАКЧАРСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**РАСПОРЯЖЕНИЕ**

20.06.2019 с. Усть-Бакчар № 15

Об утверждении технического проекта систем защиты

для информационных систем персональных данных

Администрации Усть-Бакчарского сельского поселения

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и для обеспечения защиты персональных данных в Администрации Усть-Бакчарского сельского поселения

1.Утвердить технического проекта систем защиты для информационных систем персональных данных Администрации Усть-Бакчарского сельского поселения согласно приложению к настоящему распоряжению.

2. Комиссии, утвержденной распоряжением Администрации Усть-Бакчарского сельского поселения от 17.12.2018 № 30а «О приведении в соответствие с требованиями Федерального закона № 152–ФЗ «О персональных данных» информационных системы персональных данных Администрации Усть-Бакчарского сельского поселения», обеспечить защиту персональных данных от актуальных угроз в соответствии с настоящим распоряжением.

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

|  |  |
| --- | --- |
| Глава Усть-Бакчарского сельского поселения | В.Н.Бессмертных |

Приложение

к распоряжению Администрации

Усть-Бакчарского сельского поселения

от 20.06.2019 № 15

Для служебного пользования

Экз. № 1

|  |
| --- |
| УТВЕРЖДАЮ |
| Глава Усть-Бакчарского сельского поселения |
| В.Н.Бессмертных |
| « » \_\_\_\_\_\_\_2019 г. |

**ТЕХНИЧЕСКИЙ ПРОЕКТ**

**СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ**

**ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ**

**ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ**

**УСТЬ-БАКЧАРСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

с. Усть-Бакчар – 2019 год

Содержание

1. [Общие положения 3](#_bookmark0)
   1. [Наименование проектируемой системы защиты персональных данных 3](#_bookmark1)
   2. [Назначение системы 3](#_bookmark4)
   3. [Перечень документов, на основании которых создается система 3](#_bookmark5)
   4. [Перечень нормативных документов, на основании которых создается система 4](#_bookmark6)
   5. [Очередность создания системы защиты 4](#_bookmark7)
   6. [Требования к системе защиты в целом 5](#_bookmark8)
   7. [Требования к численности и квалификации обслуживающего персонала 6](#_bookmark9)
   8. [Требования к системе защиты персональных данных в соответствии с требуемым уровнем защищенности информационной системы персональных данных 6](#_bookmark10)
2. [Решения по составу СЗПДн Администрации 10](#_bookmark11)
   1. [Решения по составу комплекса программно-технических средств относительно требований к подсистемам СЗПДн Администрации 10](#_bookmark12)
   2. [Соответствие актуальных угроз и мер, принимаемых для обеспечения безопасности персональных данных 11](#_bookmark13)
   3. [Требование по численности, квалификации, функциям и режимам работы персонала 13](#_bookmark14) [2.4 Режим функционирования 14](#_bookmark15)

Термины и сокращения...............................................................................................................16

# 1 Общие положения

# Наименование проектируемой системы защиты персональных данных

* + 1. Полное наименование проектируемой системы защиты: система защиты персональных данных информационных систем персональных данных Администрации Усть-Бакчарского сельского поселения.
    2. Условное обозначение систем защиты: СЗПДн Администрации.

# Назначение системы

СЗПДн Администрации предназначена для обеспечения безопасности персональных данных (ПДн) при их обработке в ИСПДн Администрации.

СЗПДн Администрации реализует следующие меры защиты ПДн:

* + - обеспечение конфиденциальности, целостности, доступности ПДн в ИСПДн, в том числе предотвращение несанкционированного и случайного доступа (НСД) к ПДн;
    - своевременное обнаружение фактов нарушения информационной безопасности в ИСПДн;
    - недопущение воздействия на технические средства обработки ПДн, в результате которого может быть нарушено их функционирование;
    - контроль за обеспечением уровня защищенности ПДн.

# Перечень результирующих документов

При проектировании СЗПДн Администрации оформляется технический проект, включающий в себя:

* + - изложение решений по комплексу организационных мер и программно- техническим (в том числе криптографическим) средствам обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям технического задания;
    - описание технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
    - план организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации.

По окончанию проектирования на основании разработанных документов вне данных работ возможен ввод в действие СЗПДн Администрации, включающий в себя следующие действия:

* + - опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе СЗПДн Администрации и отработки технологического процесса обработки (передачи) информации;
    - приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком.

# Перечень нормативных документов, на основании которых создается система

СЗПДн Администрации создается на основании следующих нормативных документов:

1. Федеральный закон от 08 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
3. Постановление Правительства Российской Федерации от 1 ноября 2012 г.

№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных заместителем директора ФСТЭК России от 15 февраля 2008 года;
3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

# Очередность создания системы защиты

В таблице 1.1 представлен порядок очередности создания СЗПДн Администрации.

Таблица 1.1 – Порядок создания СЗПДн Администрации

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование работ | Результат выполнения работ |
| 1 | Разработка и актуализация организационно- распорядительных документов, необходимых для обеспечения безопасности ПДн. | * Проекты организационно-распорядительных документов. |
| 2 | Внедрение системы защиты персональных данных в ИСПДн. | * Поставка программно-аппаратных средств защиты информации. * Установка и настройка СЗИ. * Проведение испытаний в соответствии с разработанной программой и методикой испытаний. * Акты ввода в эксплуатацию технических средств защиты. |

# Требования к системе защиты в целом

К СЗПДн Администрации предъявляются следующие общие требования:

* + - СЗПДн Администрации должна представлять собой согласованный комплекс организационных мероприятий, программных, технических и программно-технических мер, направленных на обеспечение информационной безопасности функционирования системы;
    - СЗПДн Администрации должна существенно затруднять реализацию потенциальных угроз информационной безопасности функционирования ИСПДн. При невозможности использования мер по предотвращению реализации угроз информационной безопасности, СЗПДн Администрации должна реализовывать механизмы, позволяющие своевременно обнаружить несанкционированную деятельность и локализовать ее источник (субъект, канал воздействия).
* СЗПДн Администрации должна отвечать требованиям нормативно-правовой базы Российской Федерации в области защиты ПДн.
* Средства защиты, используемые при построении СЗПДн, должны обеспечивать необходимый уровень защиты информации, не снижая, при этом, надежности технологий обработки информации и не оказывая существенного влияния на производительность средств вычислительной техники, входящих в ИСПДн.

Проектные решения должны предусматривать план мероприятий по внедрению средств защиты информации.

# Требования к численности и квалификации обслуживающего персонала

Для сопровождения СЗПДн Администрации достаточно одного специалиста, выполняющего функции администратора безопасности.

Администратор безопасности Администрации должен обладать знаниями в сфере информационных технологий, в объеме необходимом для администрирования узлов автоматизированных систем, сетевого и коммуникационного оборудования, а также знаниями и навыками администрирования средств защиты информации.

* 1. **Требования к системе защиты персональных данных в соответствии с требуемым уровнем защищенности информационной системы персональных данных**

Для ИСПДн «Бухгалтерия и кадры», необходимо обеспечить **четвертый уровень**

**защищенности**, так как:

* + - для данных информационных системы актуальны угрозы 3-го типа;
    - информационные система обрабатывает иные категории персональных данных субъектов ПДн, являющихся сотрудниками оператора.

Так же, для ИСПДн «Госзакупки»,«Реестры и списки», «ВИР Регистр МО» необходимо обеспечить **четвертый уровень** защищенности ПДн, так как:

* + - для информационных систем актуальны угрозы 3-го типа (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении);
    - системы обрабатывает иные категории персональных данных субъектов ПДн, не являющихся сотрудниками оператора, в количестве до 100 000 записей для каждой ИСПДн.

При этом СЗПДн Администрации должна обеспечить защиту ПДн для данных ИСПДн от следующих актуальных угроз:

* + - угроза несанкционированного копирования информации, обрабатываемой в ИСПДн;
    - угроза разглашения (публикации) защищаемой информации, обрабатываемой в ИСПДн;
    - угроза разглашения (публикации) состава и конфигурации средств защиты ПДн;
    - угроза несанкционированного уничтожения защищаемой информации, обрабатываемой в ИСПДн;
    - угроза несанкционированной модификации защищаемой информации, обрабатываемой в ИСПДн;
    - угроза нарушения функционирования и отказ средств хранения информации;
    - угроза нарушения функционирования и отказ средств защиты информации;
    - угроза внедрения (классического) программного вируса;
    - угроза внедрения программной закладки по сети;
    - угроза внедрения (классического) программного вируса по сети;
    - угроза сканирования сети;
    - угроза выявления паролей;
    - угроза удаленного запуска приложений путем распространения файлов, содержащих несанкционированный исполняемый код.

Так же, для обеспечения **4 уровня защищенности** персональных данных, требуется применение:

* + - средств вычислительной техники не ниже 6 класса;
    - систем обнаружения вторжений и средств антивирусной защиты не ниже 6

класса;

* межсетевые экраны не ниже 5 класса.

В таблице 1.2 представлен перечень адаптированных и уточненных мер защиты для обеспечения защиты ПДн в соответствии с приказом № 21 ФСТЭК России .

Таблица 1.2 – Требуемые меры защиты в соответствии с приказом № 21 ФСТЭК России

|  |  |  |
| --- | --- | --- |
| Условное обозначение | Меры защиты информации в информационных системах (ИС) | Требование приказа (+) /  доп. мера |
| 4 УЗ |
| **I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | |
| 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 | + |
| **II. Управление доступом субъектов доступа к объектам доступа (УПД)** | | |
| 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) пользователей, администраторов и лиц, обеспечивающих  функционирование информационной системы | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной  системы | + |

|  |  |  |
| --- | --- | --- |
| Условное обозначение | Меры защиты информации в информационных системах (ИС) | Требование приказа (+) /  доп. мера |
| 4 УЗ |
| 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 | Доп. мера |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной  техники | – |
| **III. Ограничение программной среды (ОПС)** | | |
| 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 | Доп. мера |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его  компонентов | Доп. мера |
| **IV. Защита машинных носителей персональных данных (ЗНИ)** | | |
| ЗНИ.1 | Учет машинных носителей персональных данных | Доп. мера |
| ЗНИ.2 | Управление доступом к машинным носителям  персональных данных | Доп. мера |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные  носители персональных данных | Доп. мера |
| ЗНИ.7 | Контроль подключения машинных носителей  персональных данных | Доп. мера |
| 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); | Доп. мера |
| **V. Регистрация событий безопасности (РСБ)** | | |
| РСБ.1 | Определение событий безопасности, подлежащих  регистрации, и сроков их хранения | + |
| РСБ.2 | Определение состава и содержания информации о  событиях безопасности, подлежащих регистрации | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях  безопасности в течение установленного времени хранения | + |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации  событий безопасности и реагирование на них | Доп. мера |
| РСБ.7 | Защита информации о событиях безопасности | + |
| **VI. Антивирусная защита (АВЗ)** | | |
| АВЗ.1 | Реализация антивирусной защиты | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных  компьютерных программ (вирусов) | + |
| **VIII. Контроль (анализ) защищенности информации (АНЗ)** | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы  и оперативное устранение вновь выявленных уязвимостей | Доп. мера |

|  |  |  |
| --- | --- | --- |
| Условное обозначение | Меры защиты информации в информационных системах (ИС) | Требование приказа (+) /  доп. мера |
| 4 УЗ |
| 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 | Доп. мера |
| АНЗ.4 | Контроль состава технических средств, программного  обеспечения и средств защиты информации | Доп. мера |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа,  полномочий пользователей в информационной системе | Доп. мера |
| **IХ. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)** | | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных  ситуаций | Доп. мера |
| 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) | Доп. мера |
| **X. Обеспечение доступности персональных данных (ОДТ)** | | |
| ОДТ.4 | Периодическое резервное копирование персональных  данных на резервные машинные носители персональных данных | Доп. мера |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных  данных (резервных копий) в течение установленного временного интервала | Доп. мера |
| **XII. Защита информационной системы, ее средств, систем связи и передачи данных** | | |
| 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 | + |
| **XIII. Защита информационной системы, ее средств, систем связи и передачи данных**  **(ЗИС)** | | |

|  |  |  |
| --- | --- | --- |
| Условное обозначение | Меры защиты информации в информационных системах (ИС) | Требование приказа (+) /  доп. мера |
| 4 УЗ |
| ЗИС.3 | Обеспечение защиты персональных данных 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 | + |
| **XIV. Выявление инцидентов и реагирование на них (ИНЦ)** | | |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов  и реагирование на них | Доп. мера |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | Доп. мера |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе  пользователями и администраторами | Доп. мера |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и  причин возникновения инцидентов, а также оценка их последствий | Доп. мера |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | Доп. мера |
| ИНЦ.6 | Планирование и принятие мер по предотвращению  повторного возникновения инцидентов | Доп. мера |
| **XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)** | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной  системы и системы защиты персональных данных | Доп. мера |
| УКФ.2 | Управление изменениями конфигурации информационной  системы и системы защиты персональных данных | Доп. мера |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение  безопасности персональных данных | Доп. мера |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы  защиты персональных данных | Доп. мера |

*России; угроз.*

*«+» – мера, обязательная к реализации в соответствии с Приказом № 21 ФСТЭК*

*«Доп. мера» – дополнительная мера, необходимая для нейтрализации актуальных*

# Решения по составу СЗПДн Администрации

* 1. **Решения по составу комплекса программно-технических средств**

**относительно требований к подсистемам**

В таблице 2 приведены способы реализации мер по обеспечению безопасности ПДн в СЗПДн Администрации.

Таблица 2.1 – Способы реализации мер по обеспечению безопасности ПДн в СЗПДн Администрации

|  |  |
| --- | --- |
| Меры по обеспечению  безопасности ПДн | Способ реализации |
| Идентификация и аутентификация  субъектов доступа и объектов доступа | * СЗИ «SecretNet Studio 8». |
| Управление доступом субъектов доступа к объектам доступа | * организационные меры; * СЗИ « SecretNet Studio 8», модуль защиты от НСД. |
| Ограничение программной среды | * организационные меры; * СЗИ « SecretNet Studio 8», модуль защиты от НСД. |
| Защита машинных носителей персональных данных | * организационные меры; * Антивирус «Dr. Web Desktop Security Suite»; * СЗИ «SecretNet Studio 8», модуль защиты   от НСД. |
| Регистрация событий безопасности | * Антивирус «Dr. Web Desktop Security Suite»; * СЗИ «SecretNet Studio 8». |
| Антивирусная защита | * организационные меры; * Антивирус «Dr. Web Desktop Security Suite». |
| Контроль (анализ) защищенности  персональных данных | * организационные меры. |
| Обеспечение целостности информационной системы и персональных данных | * организационные меры; * СЗИ «SecretNet Studio 8», модуль защиты от НСД. |
| Обеспечение доступности персональных  данных | * организационные меры. |
| Защита технических средств | * организационные меры. |
| Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз  безопасности персональных данных (далее - инциденты), и реагирование на них | * организационные меры. |
| Управление конфигурацией  информационной системы и системы защиты персональных данных | * организационные меры. |

# 2.1 Соответствие актуальных угроз и мер, принимаемых для обеспечения безопасности персональных данных

В таблице 2.2 представлены угрозы, определенные как актуальные для ИСПДн, и меры, необходимые для обеспечения безопасности ПДн, обрабатываемых в данных

ИСПДн (пояснение – если угрозы для разных ИСПДн совпадают – меры противодействия так же совпадают).

Таблица 2.2 – Соответствие актуальных угроз и мер, принимаемых для обеспечения безопасности персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| **Актуальная угроза** | **Организационные меры** | **Технические меры** | **Меры в соотв. приказом ФСТЭК**  **№21** |
| Угроза | * Разработка инструкций пользователя ИСПДн; * Разработка соглашения сотрудника о неразглашении сведений конфиденциального характера; * Инструктаж пользователей об ответственности за нарушение правил работы с ПДн; | – СЗИ «SecretNet | ИАФ.1, ИАФ.3-5,  УПД.1-6, УПД.10, ОПС.2-3,  ОДТ.4-5,  ЗНИ.1-2,  ЗНИ.6-8,  РСБ.1-3, РСБ.5,  РСБ.7,  ЗИС.2, ЗТС.2-3,  АНЗ.1-2,  ИНЦ.1-6, УКФ.1-4 |
| несанкционированного | Studio 8», модуль |
| копирования информации, | защиты от НСД; |
| обрабатываемой в ИСПДн; |  |
| Угроза разглашения |  |
| (публикации) защищаемой |  |
| информации, |  |
| обрабатываемой в ИСПДн; |  |
| Угроза разглашения |  |
| (публикации) состава и |  |
| конфигурации средств |  |
| защиты ПДн; |  |
| Угроза | * Разработка регламента резервирования и восстановления защищаемой информации; * Разграничение доступа пользователей к ПДн; * Инструктаж пользователей об ответственности за нарушение правил работы с ПДн; |  |
| несанкционированного |  |
| уничтожения защищаемой |  |
| информации |  |
| обрабатываемой в ИСПДн; |  |
| Угроза |  |
| несанкционированной |  |
| модификации защищаемой |  |
| информации |  |
| обрабатываемой в ИСПДн; |  |
|  | * Резервирование данных на носитель, хранимый отдельно от элементов ИСПДн; * Разработка регламента действий пользователя и администратора на случай нештатных ситуаций; * Хранение установочных комплектов ПО для оперативного восстановления работоспособности ИСПДн и СЗПДн |  | АНЗ.1-5, |
| Угроза нарушения функционирования и отказ средств хранения  информации; | – | ОЦЛ.3-4,  ОДТ.4-5,  ИНЦ.1-6, УКФ.1-4 |
| Угроза нарушения |  |  |
| функционирования и отказ  средств защиты | – |  |
| информации; |  |  |
|  | – Разработка регламента | – СЗИ «SecretNet | ОПС.2-3, |
| Угроза внедрения (классического) программного вируса | антивирусной защиты;  – Разработка регламента действий пользователя и администратора на случай | Studio 8», модуль защиты от НСД и модуль  межсетевого | ЗНИ.6-7,  АВЗ.1-2, АНЗ.1, СОВ.1-2 |
|  | нештатных ситуаций; | экранирования; |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | * Разработка регламента использования электронной почтой; * Разработка регламента использования сети Интернет; | – Антивирус «Dr. Web Desktop  Security Suite» |  |
| Угроза внедрения программной закладки по сети; | * Антивирус «Dr. Web Desktop Security Suite »; * СЗИ «SecretNet Studio 8», модуль межсетевого экранирования; | УПД.3, АВЗ.1-2, АНЗ.1,  ЗИС.16 |
| Угроза внедрения (классического) программного вируса по  сети; | УПД.3, АВЗ.1-2, АНЗ.1,  ЗИС.16 |
| Угроза выявления паролей; | * Разработка регламента парольной защиты; * Разработка регламента действий пользователя и администратора на случай нештатных ситуаций; | * Антивирус «Dr. Web Desktop Security Suite»; * СЗИ «SecretNet Studio 8», модуль защиты от НСД и модуль   межсетевого экранирования; | ИАФ.4-5, УПД1, УПД.3, АВЗ.1-2,  АНЗ.1-5, ЗИС.16 |
| Угроза удаленного запуска приложений путем распространения файлов, содержащих несанкционированный исполняемый код; | * Разработка инструкции пользователя ИСПДн; * Разработка регламента антивирусной защиты; * Разработка регламента использования электронной почтой; * Разработка регламента использования сети Интернет; | * Антивирус «Dr. Web Desktop Security Suite»; * СЗИ «SecretNet Studio 8», модуль межсетевого экранирования; | УПД.3, АВЗ.1-2,  АНЗ.1-5, ЗИС.16 |
| Угроза удаленного запуска приложений путем использования возможностей удаленного управления системой | * Разработка инструкции пользователя ИСПДн; * Разработка регламента антивирусной защиты; * Разработка регламента использования электронной почтой; * Разработка регламента использования сети Интернет | * Антивирус «Dr. Web Desktop Security Suite»; * СЗИ «SecretNet Studio 8» и модуль   межсетевого экранирования; | УПД.3, АВЗ.1-2,  АНЗ.1-5, ЗИС.16 |

# Требование по численности, квалификации, функциям и режимам работы персонала

Для сопровождения СЗПДн Администрации достаточно одного специалиста, выполняющего обязанности администратора информационной безопасности. На данное должностное лицо могут быть возложены функции администратора безопасности по организации работ по использованию средств криптозащиты информации, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением требований по безопасности.

Основными функциями администратора информационной безопасности в Администрации являются:

* + - администрирование ИСПДн, функционирующих в Администрации;
    - администрирование средств и систем защиты персональных данных в ИСПДн, функционирующих в Администрации;
    - контроль за функционированием СЗПДн Администрации;
    - контроль выполнения требований законодательства по защите персональных данных в Администрации;

Администратор информационной безопасности должен обладать знаниями в сфере информационных технологий, в объеме, необходимом для администрирования узлов автоматизированных систем, сетевого и коммуникационного оборудования, а также знаниями и навыками администрирования средств защиты информации.

# Режим функционирования

Нормальные режим функционирования.

В нормальном режиме функционирования системы:

* + - программное обеспечение и технические средства пользователей и администратора системы обеспечивают возможность функционирования в течение рабочего дня (с 08:00 до 19:00) пять дней в неделю;
    - исправно работает оборудование, составляющие комплекс технических средств;
    - исправно работает системное, прикладное и прочее программное обеспечение системы.

Режим отказа подсистемы СЗПДн.

Под режимом отказа подсистемы СЗПДн подразумевается отказ какой-либо из подсистем СЗПДн, ставящий под угрозу ПДн, при этом отказ рассматривается в отдельности для каждого АРМ и для сервера.

В случае отказа какой-либо подсистемы СЗПДн АРМ необходимо прекратить работу персонала на данном АРМ, отключить его питание, и связаться с организацией, оказывающей техническую поддержку СЗПДн. Прерывание работ сервера и остальных АРМ не требуется.

# Размещение комплекса технических и программных средств с учетом выполнения требований

Всего, во всех ИСПДн Администрации входят 8 АРМ и 1 Сервер. Сводный перечень требуемых средств защиты информации представлен в таблице 2.3.

Таблица 2.3 – Сводный перечень требуемых средств защиты информации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование | Кол-  во | Место  установки | Сертификат |
| 1. | Система защиты информации «SecretNet  Studio 8», включая: Модуль защиты от НСД; Модуль межсетевого экранирования. | 19 | АРМ | Сертификат соответствия ФСТЭК России  № 3675  Выдан 12.12.2016 г.  Действителен до 12.12.2019 г. |
| 2. | Антивирусное ПО  «Dr. Web Desktop Security Suite» | 22 | АРМ | Сертификат соответствия ФСБ России  № СФ/СЗ-0050 Выдан 05.06.2015 г.  Действителен до 30.06.2018 г. |

# Мероприятия по подготовке объекта автоматизации к вводу системы в действие

1. Перед установкой СЗПДн Администрации необходимо произвести ознакомление пользователей и администратора ИСПДн с документами, регламентирующими их работу в ИСПДн.
2. Установка элементов СЗПДн сопровождается актами установки и настройки средств защиты информации.
3. Проведение аттестационных испытаний

Аттестационные испытания ОТСС ИСПДн не требуются, так как угрозы утечки информации по каналам ПЭМИН были признаны неактуальными в соответствии с

«Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержденной Заместителем директора ФСТЭК России 14 февраля 2008 г.).

# Перечень принятых сокращений и обозначений

В данном документе применяются следующие термины и сокращения: АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных; НСД – несанкционированный доступ;

ОТСС – основные технические средства и системы; ПДн – программное обеспечение;

СЗИ – средства защиты информации;

СЗПДн – система защиты персональных данных; ТС – технические средства;

ФСБ России (ФСБ) - Федеральная служба безопасности Российской Федерации;

ФСТЭК России (ФСТЭК) - Федеральная служба по техническому и экспортному контролю.