П О Л И Т И К А
безопасности персональных данных
ООО «Тюмень Водоканал»

Оглавление

Список терминов и определений 3

1. Общие положения 4

2. Методы обеспечения безопасности ПДн и план работ по защите ПДн, обрабатываемых в ИСПДн Организации 5

3. Требования по обеспечению безопасности персональных данных 11

4. Пользователи ИСПДн 22

5. Требования к персоналу по обеспечению безопасности персональных данных 24

6. Должностные обязанности пользователей ИСПДн 26

7. Ответственность сотрудников ИСПДн Организации 27

Список терминов и определений

Организация – ООО «Тюмень Водоканал».

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

АРМ – автоматизированное рабочее место.

СЗПДн – система защиты персональных данных.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

1. Общие положения

Настоящий документ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Политика разработана в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требования к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет порядок защиты персональных данных, обрабатываемых в Организации.

1.1. Цель политики.

Определить требования безопасности к персональным данным, обрабатываемым в информационных системах персональных данных Организации, с целью предотвращения любого несанкционированного доступа.

Критичным фактором безопасности ПДн является организация эффективного контроля доступа к ПДн, обрабатываемых в информационных системах персональных данных. Отсутствие адекватного контроля доступа может вести к несанкционированному доступу к ИСПДн Организации.

1.2. Область применения.

Требования настоящей Политики распространяются на всех сотрудников Организации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2. Методы обеспечения безопасности ПДн и план работ по защите ПДн, обрабатываемых в ИСПДн Организации

2.1. Состав и содержание мер по обеспечению безопасности ПДн

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- 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).
- 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 за соблюдением этих правил.
- 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.
- Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.
- 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.
- 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.
- Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.
- Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных,

обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

- Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.
- Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.
- Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, 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.
- Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, 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 персональных данных, представленных в виде информативных электрических сигналов и физических полей.
- Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.
- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.
- Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Для реализации указанных методов и способов защиты информации могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

Для защиты ПДн, представленной в виде информативных электрических сигналов и физических полей могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Возможные методы и способы защиты ПДн, представленных в виде акустической (речевой) информации, заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

2.2. Принципы и способы определения актуальных угроз безопасности ПДн

Для выбора и реализации мер по обеспечению безопасности ПДн в информационной системе Организации назначается ответственный по защите информации в информационных системах персональных данных.

Выбор и реализация мер по обеспечению безопасности ПДн в ИСПДн осуществляются на основе, определяемых в Организации, угроз безопасности персональных данных (модель угроз) и в зависимости уровня защищенности ПДн, определенного в соответствии с Постановлением Правительства от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модель угроз разрабатывается на основе следующих методических документов:

- Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;
- Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России.

Модель угроз персональным данным составляется ответственным по защите ПДн и утверждается руководителем Организации.

Периодичность пересмотра модели угроз для каждой ИСПДн определена в пункте 2.4. данного документа.

2.3. Определение уровня защищенности ПДн

При обработке персональных данных в информационных системах устанавливаются уровни защищенности ПДн в соответствии с Постановлением Правительства от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При определении уровня защищенности ПДн, при их обработке в ИСПДн учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- тип угроз безопасности ПДн, актуальных для информационной системы;
- проверяется условие принадлежности ПДн сотрудникам оператора ПДн или иным субъектам, не являющихся сотрудниками оператора.

По результатам анализа исходных данных информационных систем персональных данных присваивается соответствующий уровень защищенности ПДн, и составляется «Акт определения уровня защищенности ПДн, при их обработке в ИСПДн», утверждаемый руководителем Организации.

Уровень защищенности персональных данных может быть пересмотрен:

- по решению ответственного по защите ПДн в Организации на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

2.4. План мероприятий по обеспечению безопасности ПДн

Для обеспечения безопасности процессов обработки персональных данных в Организации, должны быть выполнены работы, в соответствии с планом, указанном ниже:

Мероприятие	**Периодичность**
Организационные мероприятия	
Обследование информационных систем персональных данных	Разовое
Определение перечня ИСПДн	Разовое
Определение обрабатываемых ПДн и объектов защиты	Разовое
Определение круга лиц участвующих в обработке ПДн	Разовое
Определение ответственности лиц участвующих в обработке	Разовое
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое
Назначение ответственных за безопасность и эксплуатацию ИСПДн	Разовое
Определение уровня защищенности ПДн для всех выявленных ИСПДн	Разовое
Установление контролируемой зоны вокруг ИСПДн	Разовое
Выбор помещений для установки аппаратных	Разовое

Мероприятие	Периодичность
средств ИСПДн в помещениях, с целью исключения НСД лиц не допущенных к обработке ПДн	
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое
Организация порядка резервного копирования и восстановления защищаемой информации на твердые носители	Разовое
Введение в действие инструкции по защите ИСПДн	Разовое
Организация информирования и обучения сотрудников о порядке обработки и защиты ПДн	Разовое
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое
Разработка положения об обработке и защите ПДн, обрабатываемых в ИСПДн	Разовое
Утверждение политики безопасности персональных данных	Разовое
Организация журнала учета обращений субъектов ПДн	Разовое
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое
Организация постов охраны для пропуска в контролируемую зону	Разовое
Инженерно-технические мероприятия	
Внедрение технической системы контроля доступа в контролируемую зону и помещения	Разовое
Внедрение технической системы контроля доступа к элементам ИСПДн	Разовое
Установка жалюзи на окнах	Разовое
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое
Мероприятия по внедрению СЗИ от НСД	
Внедрение системы защиты от НСД на рабочих станциях и серверах	Разовое
Внедрение системы антивирусной защиты	Разовое
Внедрение средств межсетевого экранирования	Разовое
Внедрение средств анализа защищенности	Разовое
Внедрение средств обнаружения вторжений	Разовое
Внедрение средств криптографической защиты	Разовое
Создание журнала внутренних проверок и	Ежемесячно

Мероприятие	Периодичность
поддержание его в актуальном состоянии	
Контроль над соблюдением режима обработки ПДн	Еженедельно
Контроль над соблюдением режима защиты	Ежедневно
Контроль над выполнением антивирусной защиты	Еженедельно
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно
Контроль за обеспечением резервного копирования	Ежемесячно
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно
Тестирование реализации правил фильтрации на МЭ, настроек системы защиты от НСД, системы защиты от вирусов, системы обнаружения вторжений и анализа защищенности	Ежемесячно
Тестирование работоспособности криптографической системы защиты информации	Ежемесячно

3. Требования по обеспечению безопасности персональных данных

Выбранные и реализованные меры по обеспечению безопасности ПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных, при их обработке в информационных системах в составе системы защиты персональных данных Организации.

Система защиты персональных данных, строится на основании:

- Акта обследования информационных систем персональных данных ООО «Тюмень Водоканал»;
- Частного технического задания на «Систему защиты персональных данных информационных систем персональных данных ООО «Тюмень Водоканал»;
- Технического проекта «системы защиты персональных данных информационных систем персональных данных ООО «Тюмень Водоканал»;
- Руководящих документов ФСТЭК и ФСБ России.

Выбранные необходимые мероприятия по защите ПДн отражаются в «Описании системы защиты персональных данных Организации».

3.1. Требования по обеспечению защиты в ИСПДн «Абонентский отдел»

Для обеспечения безопасности персональных данных в ИСПДн, необходимо реализовать следующие меры:

- Идентификация и аутентификация пользователей являющихся работниками оператора
- Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
- Защита обратной связи при вводе аутентификационной информации
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
- Ограничение неуспешных попыток входа в информационную

систему (доступа к информационной системе)
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
- Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- Регламентация и контроль использования в информационной системе технологий беспроводного доступа
- Регламентация и контроль использования в информационной системе мобильных технических средств
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
- Обеспечение доверенной загрузки средств вычислительной техники
- Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
- Защита информации о событиях безопасности
- Реализация антивирусной защиты
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
- Обнаружение вторжений
- Обновление базы решающих правил
- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
- Контроль установки обновлений программного обеспечения. включая обновление программного обеспечения средств защиты информации
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
- Контроль состава технических средств, программного обеспечения и средств защиты информации
- Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе
- Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
- 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)

- Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
- Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
- 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
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
- 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
- Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
- Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных
- Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
- Защита беспроводных соединений, применяемых в информационной системе
- Определение лиц, ответственных за выявление инцидентов и реагирование на них
- Обнаружение, идентификация и регистрация инцидентов
- Своевременное информирование лиц. ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
- Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
- Принятие мер по устранению последствий инцидентов
- Планирование и принятие мер по предотвращению повторного возникновения инцидентов
- Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
- Управление изменениями конфигурации информационной системы и системы защиты персональных данных
- 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
- Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

Для обеспечения установленного уровня защищенности персональных данных, при использовании сертифицированных по требованиям безопасности информации СЗИ, применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3;

В ИСПДн все применяемое программное обеспечение средств защиты информации, должно соответствовать 4 уровню контроля отсутствия недекларированных возможностей, согласно РД ФСТЭК России.

3.2. Требования по обеспечению защиты в ИСПДн «1С»

Для обеспечения безопасности персональных данных в ИСПДн, необходимо реализовать следующие меры:

- Идентификация и аутентификация пользователей являющихся работниками оператора
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
- Защита обратной связи при вводе аутентификационной информации
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
- Разрешение (запрет) действий пользователей, разрешенных до

идентификации и аутентификации
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- Регламентация и контроль использования в информационной системе технологий беспроводного доступа
- Регламентация и контроль использования в информационной системе мобильных технических средств
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
- Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
- Защита информации о событиях безопасности
- Реализация антивирусной защиты
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
- Контроль установки обновлений программного обеспечения. включая обновление программного обеспечения средств защиты информации
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
- Контроль состава технических средств, программного обеспечения и средств защиты информации
- 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
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
- 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
- Защита беспроводных соединений, применяемых в информационной системе
- Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных

- Управление изменениями конфигурации информационной системы и системы защиты персональных данных
- 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
- Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

Для обеспечения установленного уровня защищенности персональных данных, при использовании сертифицированных по требованиям безопасности информации СЗИ, применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты;
- межсетевые экраны не ниже 3 класса;

3.3. Порядок организации доступа к ИСПДн

Все пользователи ИСПДн должны иметь доступ к ресурсам ИСПДн только в соответствии с разрешениями, установленными в «Матрице доступа пользователей к ресурсам ИСПДн».

Организация доступа нового пользователей к ресурсам ИСПДн осуществляется следующим образом:

1. Согласование доступа пользователя к ресурсам ИСПДн и добавление пользователя в «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн»;
2. Ознакомление пользователя с «Положением об обработке и защиты ПДн в Организации» и истребование с пользователя подписания «Соглашения о неразглашении ПДн»;
3. Создание учетной записи пользователя и организация доступа в соответствии с разрешениями, зафиксированными в «Матрице доступа пользователей к ресурсам ИСПДн».

При необходимости удаления доступа пользователя к ресурсам ИСПДн (в случаях увольнения сотрудника и т.д.) необходимо заблокировать (или удалить) учетную запись пользователя и откорректировать «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн».

3.4. Порядок обработки инцидентов безопасности

Порядок обработки инцидентов безопасности ПДн описан в «Инструкции по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ИСПДн».

3.5. Порядок выполнения процедур резервного копирования

Порядок процедур резервного копирования ПДн описан в «Инструкции по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ИСПДн».

3.6. Порядок организации криптографической защиты ПДн в Организации

При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе осуществляется:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;
- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;
- обучение лиц, использующих криптосредства, работе с ними;
- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);
- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:
    - индекса, условного наименования и регистрационных номеров используемых криптосредств;
    - соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;
    - соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;
    - выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3.6.1. Требования по криптографической защите информации

При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи **криптоключей не допускается,** за исключением специально организованных систем с децентрализованным снабжением криптоключами.

Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, **подлежат учету с использованием индексов или условных наименований** и регистрационных номеров.

Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы **подлежат поэкземплярному учету**.

Единицей поэкземплярного учета ключевых **документов считается ключевой носитель многократного использования**, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов **должны быть выданы под расписку** в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

Ответственный пользователь **криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет**, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны **регистрироваться в техническом (аппаратном) журнале**, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией.

Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только **между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку** в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, **исключающих бесконтрольный доступ к ним**, а также их непреднамеренное уничтожение.

Пользователи криптосредств предусматривают также раздельное **безопасное хранение действующих и резервных ключевых документов**, предназначенных для применения в случае компрометации действующих ключевых документов.

Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы **средствами контроля за их вскрытием** (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической

возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со **специально выделенными в Организации ответственными пользователями криптосредств** и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

Эксплуатационную и техническую документацию к **криптосредствам можно пересылать заказными или ценными почтовыми отправлениями**.

Для пересылки криптосредств и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. **Криптосредства пересылают отдельно от ключевых документов к ним**. На упаковках указывают название Организации или ответственного пользователя криптосредств, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

До первоначальной высылки (или возвращения) **адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей**, которыми они могут быть опечатаны.

Для пересылки криптосредств, эксплуатационной и технической документации к ним, ключевых документов следует **подготовить сопроводительное письмо, в котором необходимо указать: что посылается и в каком количестве**, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

Полученные упаковки **вскрывает только ответственный пользователь криптосредств**, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями криптосредства и ключевые документы до получения указаний от отправителя применять не разрешается.

При обнаружении **бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю** для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем криптосредств только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

Неиспользованные или выведенные из действия ключевые документы **подлежат возвращению ответственному пользователю криптосредств** или по его указанию должны быть уничтожены на месте.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам **уничтожают путем сжигания или с помощью любых бумагорезательных машин**.

Криптосредства уничтожают (утилизируют) по решению Организации, владеющей криптосредствами, и с уведомлением организации, за организацию поэкземплярного учета криптосредств.

Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом **криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам** процедура удаления программного обеспечения криптосредств и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), р**азрешается использовать после уничтожения криптосредств без ограничений**. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в

криптосредствах или иных дополнительных устройствах **уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале**.

Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях недостачи, **непредъявления ключевых документов**, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации ключевых документов организуют и осуществляют сотрудники Организации.

Изготовлять ключевые документы из исходной ключевой информации могут ответственные пользователи криптосредств, применяя штатные криптосредства, если такая возможность предусмотрена эксплуатационной и технической документацией к криптосредствам.

4. Пользователи ИСПДн

В Организации можно выделить следующие группы пользователей ИСПДн, участвующих в обработке и хранении ПДн:

- Администратор защиты;
- Операторы ИСПДн;
- Программисты.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в матрице доступа пользователей к ресурсам ИСПДн.

4.1 Администратор защиты

Администратор защиты, сотрудник Организации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент ИСПДн.

Администратор защиты обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- имеет права доступа к конфигурированию технических средств сети.

Администратор защиты уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор ИСПДн) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Организации.

4.2 Операторы ИСПДн

Оператор ИСПДн, сотрудник Организации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

4.3 Программисты

Программисты (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Организации, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

5. Требования к персоналу по обеспечению безопасности персональных данных

Все сотрудники Организации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями положения по обработке и обеспечению безопасности персональных данных, обрабатываемых в Организации.

Сотрудники Организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Организации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Организации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам, а также бывшим сотрудникам, запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Организации, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Организации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Организации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Сотрудники Организации, использующие криптосредства, допускаются к работе с ними по решению, утверждаемому руководителем Организации. При наличии двух и

более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

При использовании криптосредств в Организации сотрудники обязаны:

- не разглашать информацию о ключевых документах;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом.

Контроль за соблюдением, выше описанных требований по защите персональных данных сотрудниками Организации, возлагается на ответственного по защите информации в ИСПДн и ответственного за эксплуатацию информационных систем персональных данных в Организации.

6. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора защиты;
- Инструкция пользователя по эксплуатации СЗИ в ИСПДн;
- Инструкция по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ПДн;
- Инструкция ответственного пользователя криптосредств по обеспечению безопасности ПДн.
- Инструкция пользователя СКЗИ.

7. Ответственность сотрудников ИСПДн Организации

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор защиты несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Организации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.