СОГЛАСОВАНО

Председатель профкома

_____ О.М. Баландина

« ___ » _____ 2018 г.

УТВЕРЖДАЮ

Директор МОУ-СОШ №1

_____ Л.П. Карманова

« ___ » _____ 2018 г.

ЭЦП

Подписан: Карманова Лидия Прокопьевна
DN: C=RU, O=МОУ-СОШ №1 г. Петровск-Забайкальский, CN=Карманова Лидия Прокопьевна, E=school-1-pzb@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г. Петровск-Забайкальский
Дата: 2022.04.15 11:58:52+09'00'

МОДЕЛЬ НАРУШИТЕЛЯ

_____

_____

2018 г.

1. СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищенном исполнении
ВИ	- виртуальная инфраструктура
ИБ	- информационная безопасность
ИВС	- информационная вычислительная сеть
ИСПДн	- информационная система персональных данных
ИС	- информационная система
МЭ	- межсетевой экран
ОС	- операционная система
ОТСС	- основные технические средства и системы
ПДн	- персональные данные
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
САЗ	- система анализа защищенности
СЗИ	- средства защиты информации
СЗПДн	- система (подсистема) защиты персональных данных
СКЗИ	- средства криптографической защиты информации
СОВ	- система обнаружения вторжений
ТС	- техническое средство
УБПДн	- угрозы безопасности персональных данных

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность персональных данных – состояние защищенности персональных данных характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Встраивание СКЗИ – процесс подключения СКЗИ к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Документированные (декларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствии с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Канал атаки – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее

контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов СКЗИ и среды функционирования СКЗИ, позволяющие:

1. модифицировать или искажать алгоритм работы криптосредств в процессе их использования;

2. модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием СКЗИ;

3. получать доступ нарушителям к хранящимся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации (сведений) – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных – действия (операции) с персональными данными включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Опубликованные возможности ПО или ТС – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.).

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как

побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователь – лицо, участвующее в эксплуатации СКЗИ или использующее результаты его функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальная защита – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

Средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

Средства криптографической защиты информации (СКЗИ) - средства шифрования, средства имитозащиты, средства кодирования, средства электронной

цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которого невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к СКЗИ.

Успешная атака – атака, достигшая своей цели.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

[4] – Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден приказом ФСТЭК России от 18 февраля 2013 г. №21;

[5] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[6] - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены 21 февраля 2008 года руководством 8 Центра ФСБ России);

[7] - Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены 21 февраля 2008 года руководством 8 Центра ФСБ России).

[8] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17.

[9] - Приказ Федеральной службы безопасности Российской Федерации "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" №378 от 10 июля 2014г.

4. ОБЩИЕ ПОЛОЖЕНИЯ

В государственной информационной системе обрабатываются персональные данные, решением комиссии классифицирована как информационная система персональных данных (далее - ИСПДн).

установлена необходимость обеспечения **2-го уровня защищенности (УЗ 2)** персональных данных.

Настоящий документ содержит анализ и описание вероятных нарушителей информационной безопасности (далее - ИБ) ИСПДн

Разработка Модели нарушителя (далее - Модель) является необходимым условием формирования и конкретизации обоснованных требований к обеспечению ИБ ИСПДн и проектирования СЗПДн.

Модель нарушителя разработана в целях:

– определения вероятных нарушителей ИБ ИСПДн;

– определения основных направлений реализации СЗПДн, обеспечивающих нейтрализацию актуальных угроз ИБ с использованием методов и способов защиты ПДн, предусмотренных в соответствии с классом ИСПДн;

– определения организационных мероприятий направленных на обеспечение ИБ ИСПДн с учетом особенностей реализации технологического процесса обработки информации в ИСПДн.

5. ОПИСАНИЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ

Всех нарушителей ИБ целесообразно разделить на две группы:

1. ***Внутренние нарушители*** – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

2. ***Внешние нарушители*** – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

В качестве основных побудительных причин действий нарушителей ИБ ПДн следует рассматривать:

– получение материальной выгоды;

– моральное удовлетворение без получения материальной выгоды;

– халатность, невнимательность, спешка;

– месть;

– деятельность, связанная с промышленным шпионажем и конкурентной борьбой субъектов рынка.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами ИСПДн. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в ИСПДн - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием ИСПДн, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств ИСПДн, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Исходя из квалификации нарушителя и его технической оснащенности, всех потенциальных нарушителей можно классифицировать по следующим критериям:

1. По уровню знаний программно-технических средств ИСПДн:

– нарушитель, знающий функциональные особенности, основные закономерности формирования массивов данных и потоков запросов к ним, а также умеющий пользоваться основными техническими средствами и системами;

– нарушитель, обладающий высоким уровнем знаний и опытом работы с программно-техническими средствами, и их обслуживания;

– нарушитель, обладающий высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

– нарушитель, знающий структуру, функции и механизм действия средств защиты информации, их сильные и слабые стороны.

2. По уровню возможностей (используемым методам и средствам):

– нарушитель, применяющий агентурные методы получения сведений;

– нарушитель, применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

– нарушитель, использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно внесены;

– нарушитель, применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

3. По времени действия:

– нарушитель, воздействующий на программно-технические средства во время их работы;

– нарушитель, воздействующий на программно-технические средства в период их неактивности (в нерабочее время, во время плановых перерывов в работе, перерывов для обслуживания и ремонта и т.п.);

– нарушитель, воздействующий на программно-технические средства как в процессе их функционирования, так и в период их неактивности.

4. По месту действия:

– нарушитель, воздействующий на программно-технические средства без доступа в контролируемую зону;

– нарушитель, воздействующий на программно-технические средства с контролируемой зоны без доступа в здания и сооружения и из-за пределов КЗ;

– нарушитель, воздействующий на программно-технические средства внутри помещений;

– нарушитель, воздействующий на программно-технические средства с рабочих мест конечных пользователей (операторов) и обслуживающего персонала;

– нарушитель, воздействующий на программно-технические средства с доступом в зону данных (баз данных, архивов и т.п.);

– нарушитель, воздействующий на программно-технические средства с доступом в зону управления средствами обеспечения безопасности.

5. По степени опасности для программно-технических средств ИСПДн определена следующая иерархия потенциальных нарушителей:

– внутренние нарушители, обладающие определенными полномочиями и имеющие физический доступ к наиболее важным узлам (сервера, устройства коммутации, и т.д.).

– внутренние нарушители, которые осуществляют деструктивные действия не из злого умысла, а по незнанию, неосторожности или из любопытства.

– внешние нарушители, которые знают внутреннюю структуру программно-технических средств и в состоянии организовать не только атаки на внешние точки, но и осуществлять более разрушительные воздействия исходя из своих знаний о программно-технических средствах, методах защиты, каналах передачи данных и т.д.

– внешние нарушители, которые будут действовать при осуществлении попыток доступа наугад, не имея уверенности в том, каков будет результат.

6. ВНУТРЕННИЙ НАРУШИТЕЛЬ

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой разрешительной системой доступа.

К внутренним нарушителям могут относиться:

1. Пользователи ИСПДн – ***категория В1***;
2. Администраторы ИСПДн - ***категория В2***;
3. Сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ОТСС ИСПДн, но не имеющие права доступа к ПДн (в т.ч. обслуживающий персонал охрана, работники инженерно-технических служб) - ***категория В3.***

Общая характеристика вероятных внутренних нарушителей ИБ ПДн приведена в Таблице 1.

Таблица 1

Категория нарушителя, обозначение	**Выполняемые функции в ИСПДн**	**Возможности**	**Степень опасности**
Зарегистрированный пользователь ИСПДн, имеющий доступ к персональным данным с персонального рабочего места (В1)	Осуществляет работу с БД (ввод, корректировка, обработка данных) в соответствии с присвоенными полномочиями	- располагает фрагментами информации о топологии ИСПДн; - знает, по меньшей мере, одно легальное имя доступа; обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству персональных данных; - располагает персональными данными, к которым имеет доступ	Средняя
Администраторы ИСПДн (В2)	Выполнение администрирования средств защиты информации, сетевой инфраструктуры ИСПДн, виртуальной инфраструктуры ИСПДн, поддержание в работоспособном состоянии технических средств ИСПДн.	Имеет непосредственный доступ к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных ИСПДн, в соответствии с установленными для них административными полномочиями	Высокая
Сотрудник, не имеющий права доступа к ПДн (В3)	Не осуществляет обработку персональных данных, не имеет регламентированного доступа к ОТСС ИСПДн	Не располагает знаниями о принципах построения и функционирования ИСПДн. Не располагает персональными данными.	Низкая

Категория нарушителя, обозначение	Выполняемые функции в ИСПДн	Возможности	Степень опасности
		Может получить доступ путем компрометации паролей или в результате халатности пользователей ИСПДн	

6.1. КАТЕГОРИЯ В1 – ЗАРЕГИСТРИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ ИСПДН

Нарушители В1 являются государственными гражданским служащими _____. Доступ нарушителей В1 необходим для выполнения ими своих должностных обязанностей, в том числе, для обработки персональных данных. Доступ к персональным данным пользователей регламентирован организационно-распорядительными документами и осуществляется с персональных рабочих мест, входящих в состав ОТСС ИСПДн.

В качестве меры доверия к данной категории пользователей выступает обязательство о неразглашении персональных данных, которое они принимают под роспись.

6.2. КАТЕГОРИЯ В2 – АДМИНИСТРАТОРЫ ИСПДН

Выделяются следующие уровни администрирования (Таблица 2):

– администратор безопасности информации;

– системный администратор.

Администраторы хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Кроме того, они имеют непосредственный доступ к серверному и коммутационному оборудованию ИСПДн. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Таблица 2. Структура администрирования ИСПДн.

№ п/п	Функции по администрированию ИСПДн	Реализуемые задачи	Примечание
1.	Администратор безопасности информации (А1)	1. Сопровождение в процессе эксплуатации СЗПДн ИСПДн подсистем ее защиты. 2. Контроль выполнения требований действующих нормативных документов по вопросам обеспечения безопасности персональных данных в ходе эксплуатации пользователями ИСПДн. 3. Руководство и контроль деятельности системных администраторов. 4. Контроль порядка допуска пользователей к работе в ИСПДн и назначения им прав по доступу к персональным данным.	Обладает правами доступа к информационным, программным и аппаратным ресурсам сети организации и средствам защиты информации.
2.	Системный администратор	1. Поддержание работоспособности и	Обладает правами

№ п/п	Функции по администрированию ИСПДн	Реализуемые задачи	Примечание
	(А2)	безотказности функционирования серверного и коммутационного оборудования ИСПДн. 2. Выбор и конфигурирование сетевых протоколов. 3. Настройка таблиц маршрутизации. 4. Определение и назначение сетевых адресов компьютерам и узлам связи. 5. Организация обеспечения бесперебойного функционирования серверов, а также информационных систем в виртуальной среде; 6. Обеспечение мониторинга состояния параметров программно-технических средств и анализ показателей использования и функционирования программно-технических средств виртуальной инфраструктуры; 7. Организация работы систем хранения данных; 8. Реализация политики разграничения доступа к ресурсам виртуальной инфраструктуры. 9. Поддержание в актуализированном состоянии перечня ролей доступа пользователей к ресурсам БД. 10. Выполнение регламентированных мероприятий по предоставлению пользователям прав доступа к работе в ИСПДн. 11. Организация и выполнения процедур резервирования БД.	доступа к серверному и сетевому оборудованию ИСПДн. Обладает правами доступа к системе управления сервером виртуализации, виртуальным машинам и системе хранения данных. Обладает правами по администрированию БД. Осуществляет свою деятельность под руководством администратора безопасности информации.

Администраторы являются привилегированными пользователями информационной системы, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств СКЗИ и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

Администратор безопасности информации (А1) исключается из числа потенциальных нарушителей как доверенное лицо, заинтересованное в соблюдении характеристик безопасности защищаемых объектов.

Системный администратор (А2) может получить непосредственный доступ к серверному, коммутационному оборудованию ИСПДн, виртуальной инфраструктуре и базам банных.

При администрировании сетевого коммутационного оборудования администратор (А2) обладает полномочиями по конфигурированию сетевых протоколов, настройке таблиц маршрутизации, назначении сетевых адресов.

В виртуальной инфраструктуре обладает широкими полномочиями по управлению виртуальными машинами (ВМ), такими, как:

- Создание, редактирование параметров и удаление ВМ;
- Приостановка и возобновление работы ВМ;
- Приостановка и завершение гостевой ОС;
- Перемещение ВМ на другой сервер и смена хранилища ВМ;
- Доступ к хранилищу ВМ;
- Редактирование различных сетевых параметров ВМ.

При администрировании виртуальной инфраструктуры, администратор (А2) имеет возможность доступа к данным, обрабатываемым внутри виртуальных машин.

При администрировании баз данных администратор А2 занимается их управлением и имеет удаленный доступ к серверам на которых установлены базы данных.

Категория администраторов А2 является работниками Центра обработки данных _____, которые осуществляют свою деятельность в соответствии с должностными инструкциями, несут личную ответственность за обеспечение безопасности ПДн. Контроль за деятельностью данной категорий администраторов, а также периодический аудит информационной безопасности в ИСПДн осуществляет администратор безопасности информации.

В качестве меры доверия к администраторам всех типов выступает обязательство о неразглашении персональных данных, которое они принимают под роспись.

Для защиты среды виртуализации в ИСПДн применяется сертифицированное СЗИ, что позволяет исключить администратора А2 из списка потенциальных нарушителей.

6.3. КАТЕГОРИЯ В3 – СОТРУДНИКИ, НЕ ИМЕЮЩИЕ ПРАВА ДОСТУПА К ПДН

К категории В3 относятся сотрудники Администрации, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся: энергетики, сантехники, уборщицы и другие лица, обеспечивающие нормальное функционирование объекта информатизации, а так же служащие (работники) Администрации.

Лица данной категории могут:

− располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;

− изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в программно-технические средства ИСПДн и

обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

Нарушителей категории В3 возможно не рассматривать в качестве потенциальных за счет реализации организационно-технических мероприятий по контролю доступа на территорию контролируемой зоны и в помещения ИСПДн (ЦОД).

7. ВНЕШНИЙ НАРУШИТЕЛЬ

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки за счет реализации мер по контролю доступа на территорию КЗ. Данный вид угроз признан неактуальным для ИСПДн в Модели угроз.

К внешним нарушителям могут относиться:

1. Посетители, имеющие разовый пропуск - ***категория Б1;***
2. Представители организаций, проводящих работы на территории ИСПДн, в том числе организации, осуществляющие поставку и гарантийное сопровождение технических средств ИСПДн - ***категория Б2;***
3. Лица, находящиеся за пределами контролируемой зоны и использующие технические средства (в том числе бывшие сотрудники – администраторы или пользователи ИСПДн) – ***категория Б3;***
4. Представители компании «_____», осуществляющей конфигурирование и настройку платформы _____ – ***категория Б4.***

Таблица 3. Характеристика внешних нарушителей

Категория нарушителя	**Квалификация**	**Техническая оснащенность**	**Степень опасности**
Посетители, имеющие разовый пропуск (Б1)	Не обладает высоким уровнем знаний в области ИТ	Не располагает знаниями о принципах построения и функционирования ИСПДн. Может получить доступ путем компрометации паролей или в результате халатности пользователей ИСПДн	Низкая
Представители организаций, проводящих работы на территории ИСПДн, в том числе организации, осуществляющие поставку и гарантийное сопровождение технических средств ИСПДн (Б2)	Обладает высоким уровнем знаний и опытом работы с программно-техническими средствами, и их обслуживания	Основное компьютерное оборудование. В некоторых случаях используется более сложная аппаратура	Средняя
Лица, находящиеся за пределами контролируемой зоны и использующие технические средства разведки (Б3)	Высокая квалификация. Опыт получен в процессе профессиональной деятельности	Технические средства перехвата информации	Высокая

Категория нарушителя	Квалификация	Техническая оснащенность	Степень опасности
Представители организации, осуществляющей конфигурирование и настройку платформы MS MS SQL Server 2012R2 (Б4)	Обладает высоким уровнем знаний и опытом работы с программно-техническими средствами, и их обслуживания	Основное компьютерное оборудование.	Средняя

Нарушителей Б1, Б2 в соответствии с классификацией, приведенной в Таблице 3, возможно не рассматривать в качестве потенциальных в силу организации надежной системы контроля доступа на территорию контролируемой зоны, а также реализации организационно-технических мероприятий, в том числе применения сертифицированных средств защиты информации.

Субъекты категории Б3 могут быть хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Субъекты категории Б4 не имеют доступ к персональным данным, но обладают возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. В качестве меры доверия к данной категории пользователей выступает государственный контракт, в котором прописана обязанность соблюдения конфиденциальности информации заказчиком.

В качестве наиболее вероятных нарушителей ИБ целесообразно рассматривать:

1. Внутренний нарушитель класса В1 (Зарегистрированный пользователь ИСПДн).

2. Внешний нарушитель класса Б3 (Лица, находящиеся за пределами контролируемой зоны и использующие технические средства).

Предполагается, что вероятность сговора групп нарушителей минимальна.

8. ПРЕДПОЛОЖЕНИЯ О ВОЗМОЖНОСТЯХ НАРУШИТЕЛЕЙ

В качестве основных уровней знаний нарушителей об ИСПДн можно выделить следующие:

1. информация о назначении и общих характеристиках ИСПДн;
2. информация, полученная из эксплуатационной документации;
3. информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

1. данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
2. сведения об информационных ресурсах ИСПДн (порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков);
3. данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
4. данные о реализованных в СЗИ принципах и алгоритмах;
5. исходные тексты программного обеспечения ИСПДн;
6. сведения о возможных каналах реализации угроз;
7. информацию о способах реализации угроз.

Предполагается, что лица категорий Б3 не владеют парольной и аутентифицирующей информацией, используемой в ИСПДн, но могут обладать чувствительной информацией об ИСПДн, включая информацию об уязвимостях технических и программных средств ИСПДн.

Лица категории Б4 имеют доступ к средствам обработки данных в ИСПДн и обладают информацией об алгоритмах и программах обработки информации в ИСПДн

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетентность нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания необходимых условий безопасности персональных данных предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

9. ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩИХСЯ У НАРУШИТЕЛЯ СРЕДСТВАХ РЕАЛИЗАЦИИ УГРОЗ

Предполагается, что нарушитель имеет:

1. аппаратные компоненты СЗПДн и среды функционирования СЗПДн;

2. доступные в свободной продаже технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Для определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, доступные в свободной продаже, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

1. средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

2. средств воздействия на источники и через цепи питания;

3. средств воздействия через цепи заземления;

4. средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории Б3.

10. ОПИСАНИЕ ОБЪЕКТОВ И ЦЕЛЕЙ РЕАЛИЗАЦИИ УГРОЗ ИБ

Основными информационными ресурсами, обрабатываемыми в ИСПДн являются следующие:

1. Целевая информация:
   - персональные данные;
2. Технологическая информация:
   - защищаемая управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
   - защищаемая технологическая информация средств доступа к системам управления ИСПДн (аутентификационная информация и др.);
   - информационные ресурсы ИСПДн на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами ИСПДн (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
   - информация о СЗПДн, их структуре, принципах и технических решениях защиты;
   - информационные ресурсы ИСПДн (базы данных и файлы), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
3. Программное обеспечение:
   - программные информационные ресурсы ИСПДн, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами ИСПДн, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств защиты.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

11. ОПРЕДЕЛЕНИЕ ТИПА НАРУШИТЕЛЯ

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу.

Различают шесть основных типов нарушителей: H_1, H_2, … , H_6. Возможности нарушителя H_{i+1} включают в себя возможности нарушителя H_i .

Нарушители типа H_1 могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны.

Нарушители типа H_1 и H_2 располагают только доступным в свободной продаже аппаратными компонентами СКЗИ и СФК.

Только нарушителям типа H_3 – H_6 могут быть известны все сети связи, работающие на едином ключе.

Дополнительные возможности нарушителей типа H_3 – H_5 по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер.

Нарушители типа H_4–H_6 могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы.

С учетом анализа автоматизированной системы, принимая во внимание организационные и технические меры по обеспечению безопасности в ИСПДн, определены наиболее вероятные нарушители.

Внутренние нарушители:

- Зарегистрированный пользователь ИСПДн – соответствует типу H_2.

Внешние нарушители:

- Лица, находящиеся за пределами контролируемой зоны и использующие технические средства – соответствует типу H_1 .

В результате определен наивысший тип внутреннего нарушителя – **H_2**, внешнего нарушителя – **H_1**. Для защиты от внутреннего нарушителя СКЗИ должно обеспечить криптографическую защиту по уровню **КС2**, для защиты от внешнего нарушителя – **КС1**.

12. ТРЕБОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ОТ ОПРЕДЕЛЕННОГО ТИПА НАРУЩИТЕЛЕЙ

Для обеспечения 2 уровня защищенности персональных данных при их обработке в ИСПДн необходимо выполнение следующих требований:

1) организация режима обеспечения безопасности помещений, в которых размещены элементы ИСПДн, должна препятствовать возможности неконтролируемого проникновения лиц, не имеющих права доступа в эти помещения.

- входные двери в помещения должны быть с замками;

- двери должны быть постоянно закрыты;

- в конце рабочего дня двери должны опечатываться печатью;

- помещение должно быть оборудовано техническими устройствами, сигнализирующими о несанкционированном вскрытии;

- должны быть, утверждены правила доступа в помещения;

- должен быть утвержден список лиц (должностей), имеющий доступ в данные помещения.

2) обеспечение сохранности носителей персональных данных.

- съемные машинные носители информации (ПДн) должны храниться в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

- должен быть обеспечен поэкземплярный учет машинных носителей персональных данных (журнал учета конфиденциальных машинных носителей информации).

3) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

Данный документ должен постоянно находиться в актуальном состоянии.

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. Необходимо для каждого из уровня значимости ПДн применение СКЗИ соответствующего класса позволяющих обеспечить безопасность ПДн при реализации атак с использованием аппаратных, программных средств.

- получения исходных данных для формирования предложений о возможностях, которые могут использоваться при создании способов, подготовки и проведении атак;

- формирования и утверждения совокупности предположений о возможностях, которые могут использоваться при проведении возможных атак, и определение на этой основе требуемого класса СКЗИ;

- использования для обеспечения требуемого уровня защищенности ПДн при их обработке в ИСПДн СКЗИ.

5) СКЗИ класса КС1 применяются для нейтрализации атак, при создании способов, подготовки проведении которых используются возможности из числа следующих:

- создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

- создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;

- проведение атаки, за пределами контролируемой зоны;

- проведение на этапах пусконаладочных работ

- проведение атак на этапе эксплуатации СКЗИ на:

  - - персональные данные;
  - - ключевую, аутентифицирующую и парольную информацию СКЗИ;
  - - программные компоненты СКЗИ;
  - - аппаратные компоненты СКЗИ;
  - - программные компоненты СФ, включая программное обеспечение BIOS;
  - - аппаратные компоненты СФ;
  - - данные, передаваемые по каналам связи;
  - - иные объекты.

- получение из находящихся в свободном доступе источников информации об информационной системе, в которой используется СКЗИ.

- применение находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ и специально разработанных АС и ПО;

- использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки

- проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;

- использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО штатных средств.

6) СКЗИ класса КС2 применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных для СКЗИ класса КС1 и не менее одной из следующих дополнительных возможностей:

- проведение атаки при нахождении в пределах контролируемой зоны;

- проведение атак на этапе эксплуатации СКЗИ на документацию на СКЗИ и компоненты СФ и помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

- получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
- - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;
- - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

- использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

- назначение сотрудника (работника), ответственного за обеспечение безопасности персональных данных в информационной системе;

- необходимо осуществлять ведение электронного журнала сообщений;

- доступ к содержанию электронного журнала сообщений должен быть возможен исключительно для сотрудников (работников) оператора, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

- необходимо утвердить и поддерживать в актуальном состоянии список лиц, допущенных к содержанию электронного журнала сообщений;

- обеспечение ИСПДн автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных;

- обеспечение ИСПДн автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не допущенных данному журналу;

- обеспечение периодического контроля работоспособности автоматизированных систем.