СОГЛАСОВАНО

Председатель профкома

_____ О.М. Баландина

« ___ » _____ 2018 г.

УТВЕРЖДАЮ

Директор МОУ-СОШ №1

_____ Л.П. Карманова

« ___ » _____ 2018 г.

МОДЕЛЬ УГРОЗ

БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

при их обработке в школе

2018 г.

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: 2022.04.20 14:03:48+09'00'

ОГЛАВЛЕНИЕ

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
ИС	- информационная система
ИСПДн	- информационная система персональных данных
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 СКЗИ 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 – 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 - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Криптографически опасная информация (КОИ) – информация о состояниях СКЗИ, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

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

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:

- модифицировать или искажать алгоритм работы СКЗИ в процессе их использования;

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

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 – 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.

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 - 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.

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).

Центр обработки данных (ЦОД) – программно-аппаратная отказоустойчивая комплексная централизованная система, обеспечивающая автоматизацию бизнес-процессов с высоким уровнем производительности и качеством предоставляемых сервисов, обеспечивающая гарантированную безотказную работу размещенной в ней системы с заданными уровнями доступности, надежности, безопасности и управляемости.

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] - Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[4] - Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012.

[5] - Приказ ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[6] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

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

4. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Модель угроз разработана по результатам обследования МОУ-СОШ №1 единой федеральной межведомственной системы учета контингента обучающихся по начальным, основным, средним образовательным программам и дополнительным общеобразовательным программам» (далее - школа), с целью формирования обоснованных требований к обеспечению безопасности информации в информационной системе.

В соответствии с Актом классификации, школа является государственной информационной системой и информационной системой персональных данных (далее - ИСПДн).

В соответствии с [2], Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

В соответствии с [5], определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе и разработка на их основе модели угроз безопасности информации является необходимым требованием на этапе формирования требований к защите информации, содержащейся в информационной системе.

Настоящая Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [7]. Кроме того, Модель угроз может быть пересмотрена по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или)

изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

5. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Школа является частью Межведомственной системы, предназначенная для учета контингента обучающихся по начальным, основным, средним образовательным программам и дополнительным общеобразовательным программ.

Целями _____ являются:

- повышение эффективности государственного и муниципального управления в сфере образования за счет использования современных информационных технологий;

- повышение качества оказания населению государственных и муниципальных услуг в электронном виде в образовательной сфере;

Задачами _____ являются:

- получение информации о контингенте обучающихся в образовательных учреждениях;

- получение оперативной информации об очередях на зачисление в образовательные учреждения, и о степени их наполнения;

- прогнозирование необходимого качества мест в образовательных учреждениях

- учет обучающихся в образовательных учреждениях;

- формирование полного набора данных об этапах обучения и достижениях обучающихся при их обучении в образовательных учреждениях, включая результаты дополнительного образования;

- получении информации о влиянии образовательного процесса на состояние здоровья обучающихся;

- повышение доступности для населения информации об образовательных учреждениях и оказываемых ими образовательных услугах через государственные информационные порталы;

- организация возможности подачи заявлений о зачислении обучающихся в дошкольные образовательные учреждения и общеобразовательные учреждения в электронном виде;

- сокращение количества документов и информации, поддерживающих предоставлению заявителями для получения государственных или муниципальных услуг в сфере образования.

В составе _____ функционируют:

Аппаратные средства:

Физический сервер:

- _____

Девять виртуальных сервера на базе:

- _____

Программные средства:

- _____

Существующая аппаратная и телекоммуникационная инфраструктура.

Инфраструктура централизованного управления вычислительными ресурсами функционирует на базе ОС _____. Сервера работают в виртуальной среде под управлением гипервизора _____.

Данные хранятся на двух узлах _____ под управлением ОС _____. Сервера узлов работают в виртуальной среде под управлением гипервизора _____. Дополнительно осуществляется репликация (дублирование) на физический _____.

Серверы подключены к высокопроизводительному стеку коммутаторов третьего уровня, образующих уровень ядра вычислительной сети Заказчика.

Система обслуживает подключения АРМ пользователей, находящихся как в пределах ИВС, так и за пределами ИВС, через защищенную сеть.

Система обеспечивает прямое информационное взаимодействие со следующими внешними информационными системами:

- федеральный сегмент;
- ИС Управления ЗАГС;
- ИС «Сервис образовательного учреждения»;
- СМЭВ
- ЕПГУ;
- ЕСИА;
- ЕСНСИ.

Серверная часть, обеспечивает консолидацию вычислительных ресурсов оборудования Центра обработки данных (далее - ЦОД), расположенного в серверном помещении информационных технологий и документальной связи.

Управление базами данных в школе осуществляется с использованием серверов базы данных _____. В качестве приложения в ИСПДн используется интернет-браузер, в качестве веб-серверов используется _____. Браузер клиента взаимодействует с веб-серверами по протоколу HTTPS, веб-сервера в свою очередь взаимодействует с приложением _____.

Перечень средств защиты информации, применяемых в ЦОД, указан в следующей таблице:

Состав СЗИ ЦОД

Тип СЗИ	Наименование	Примечание
Средство защиты информации от несанкционированного доступа (СЗИ от НСД)		
Средство защиты от НСД виртуальной инфраструктуры		
Средство межсетевого экранирования		
Средство антивирусной защиты		
Средство анализа защищенности		
Средство криптографической защиты информации		
Средство обнаружения вторжений		

Состав ТС ИСПДн

В таблице указан перечень используемых ТС:

№ п/п	Наименование ТС
1	Серверы, обрабатывающие ПДн
2	Рабочие станции пользователей
3	Сетевое оборудование участвующее в передаче ПДн по ИСПДн
4	Кабели питания серверов и рабочих станций, обрабатывающих ПДн
5	Линии вспомогательных средств и систем, размещенных в помещениях с техническими средствами, обрабатывающими ПДн
6	Принтеры (локальные и сетевые) и прочие печатающие устройства
7	Съемные носители информации
8	Система резервного питания (ИБП)

Состав ПО ИСПДн

В таблице указан перечень используемого ПО:

№ п/п		Наименование
1	ОС для серверов	
2	ОС для рабочих станций	
3	СУБД	
6	Программы	
7	Архиваторы	

6. ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПДН

Настоящий раздел составлен в соответствии с [6] и [7]. В разделе определяются актуальные угрозы безопасности персональных данных.

Каждая угроза, связанная с несанкционированным доступом, определяется из совокупности факторов: *<источник угрозы, уязвимость, способ реализации, объект воздействия, деструктивное действие>*.

Каждая угроза, связанная с утечкой информации по техническим каналам, определяется на основании факторов: *<источник угрозы, носитель ПДн, канал утечки>*. По результатам обследования ИСПДн определено наличие мер и предпосылок для возможных угроз.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

6.1. ИСХОДНЫЕ ДАННЫЕ

а) Категория обрабатываемых ПДн:

В ИСПДн обрабатываются **специальные** категории персональных данных – обрабатываются персональные данные, касающиеся, состояния здоровья, субъектов ПДн.

б) Объем обрабатываемых ПДн:

В ИСПДн одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных.

в) Тип актуальных угроз:

Угрозы **третьего** типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

г) Структура:

По структуре ИСПДн представляет собой **распределенную** информационную систему - комплекс АРМ и (или) локальных информационных систем, объединенных в единую информационную систему с использованием технологии удаленного доступа.

д) Масштаб:

Информационная система имеет **региональный** масштаб и функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

е) Наличие подключений к сетям общего пользования:

В ИСПДн имеется доступ к сетям международного информационного обмена (сеть Интернет).

ж) Режим обработки ПДн:

В ИСПДн режим обработки ПДн многопользовательский с разными правами доступа пользователей.

з) Местонахождение технических средств:

Все технические средства находятся в пределах Российской Федерации.

и) Классификация:

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах» для государственной информационной системы единой федеральной межведомственной системы учета контингента обучающихся по начальным, основным и средним образовательным программам и дополнительным общеобразовательным программам» установлен **второй класс защищенности (К2)**.

В соответствии с постановлением Правительства № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных школы классифицирована как информационная система персональных данных и установлена необходимость обеспечения **2-го уровня защищенности персональных данных** при их обработке в информационной системе.

6.2. ОПРЕДЕЛЕНИЕ ИСХОДНОЙ ЗАЩИЩЕННОСТИ

Информационная система персональных данных _____ имеет следующие технические и эксплуатационные характеристики:

1) Территориальное размещение ИСПДн – распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом. Уровень защищенности - *низкий*.
2) Наличие соединения с сетями связи общего пользования - ИСПДн, имеющая одноточечный выход в сеть общего пользования. Уровень защищенности - *средний*.

3) Встроенные (легальные) операции с записями баз персональных данных – модификация, передача. Уровень защищенности - *низкий*.

4) Разграничение доступа к персональным данным - ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн. Уровень защищенности - *средний*.

5) Наличие соединений с другими базами персональных данных иных ИСПДн – интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн). Уровень защищенности - *низкий*.

6) Уровень обобщения (обезличивания) персональных данных - ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю организации. Уровень защищенности - *средний*.

7) персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки - ИСПДн, предоставляющая часть ПДн. Уровень защищенности – *средний.*

Определение исходной степени защищенности:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70 % характеристик соответствуют уровню «высокий»;

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПДн соответствуют уровню не ниже «средний»;

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	0	0%
2	Средний	4	57%
3	Низкий	3	43%

В соответствии с полученными данными устанавливается **низкий показатель исходной защищенности**, значение коэффициента $\mathbf{Y_1=10}$.

6.3. ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ПДн

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

6.3.1. Угрозы утечки информации по техническим каналам

Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы **– *маловероятна*.**

Угрозы утечки видовой информации.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

Бесконтрольное пребывание посторонних лиц в здании не допускается, организован пропускной режим. В помещении ЦОДа, где размещаются сервера ИСПДн,

нет окон, установлена металлическая дверь, доступ разрешен только ограниченному кругу лиц.

В зданиях органов государственной власти также организован пропускной режим. На окнах используются жалюзи и занавески. Доступ посторонних лиц в помещения, в которых производится обработка ПДН, ограничен.

1. Реализация угрозы внешним нарушителем из-за пределов контролируемой зоны

Вероятность реализации угрозы – ***низкая вероятность.***

2. Реализация угрозы внешним нарушителем в пределах контролируемой зоны

Вероятность реализации угрозы – ***низкая вероятность.***

3. Реализация угрозы внутренним нарушителем

Вероятность реализации угрозы – ***средняя вероятность.***

Угрозы утечки информации по каналам ПЭМИН.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угроза утечки информации, содержащей ПДн, по каналу ПЭМИН возможна, за счет перехвата техническими средствами разведки за пределами контролируемой зоны ПЭМИН, возникающих при обработке ПДн средствами вычислительной техники ИСПДн. Наиболее опасным режимом работы средств вычислительной техники является вывод информации на экран монитора автоматизированного рабочего места оператора (пользователя) ИСПДн.

В качестве наиболее вероятного нарушителя, ведущего разведку ПЭМИН, необходимо рассматривать внешнего нарушителя действующего за пределами контролируемой зоны.

Серверы ИСПДн расположены в охраняемом здании, в выделенном помещении, куда имеет доступ ограниченный круг лиц. Бесконтрольное пребывание посторонних лиц в здании не допускается. Расстояние от технических средств, расположенных в серверном помещении, до границ контролируемой зоны (внешние стены здания) составляет не менее 5 метров.

В зданиях органов государственной власти также организован пропускной режим. Доступ посторонних лиц в помещения, в которых производится обработка ПДн, ограничен.

Вероятность реализации угрозы – ***низкая вероятность.***

6.3.2. Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

Угрозы НСД в ИСПДн путем физического доступа:

Кража ПЭВМ.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн.

В помещениях ИСПДн, установлена охранно-пожарная сигнализация, подключенная к пульту __01_____. В серверном помещении есть окона, установлена деревянная дверь, доступ разрешен только ограниченному кругу лиц. Бесконтрольное пребывание посторонних лиц в здании не допускается. Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора или администратора информационной безопасности.

В зданиях органов государственной власти организован пропускной режим. Доступ посторонних лиц в помещения, в которых производится обработка ПДн, ограничен.

Переносные компьютеры для обработки ПДн в ИСПДн не используются.

Вероятность реализации угрозы **– *низкая вероятность*.**

Кража носителей информации, в т.ч. содержащих образы виртуальных машин

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации. В результате возможно несанкционированное копирование разделов системы хранения данных штатными средствами на съемные устройства хранения.

В помещениях ИСПДн, установлена охранно-пожарная сигнализация, подключенная к пульту __01_____. В серверном помещении есть окона, установлена деревянная дверь, доступ разрешен только ограниченному кругу лиц. Бесконтрольное пребывание посторонних лиц в здании не допускается. Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора или администратора информационной безопасности.

В зданиях органов государственной власти организован пропускной режим. Доступ посторонних лиц в помещения, в которых производится обработка ПДн, ограничен. .

Переносные компьютеры для обработки ПДн в ИСПДН не используются.

Доступ к резервным копиям базы данных имеет только администратор баз данных ИСПДн.

Защищаемая информация обрабатывается и хранится только на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

Для обработки ПДн внешние носители информации не используются.

Вероятность реализации угрозы – ***низкая вероятность***.

Кража ключей и атрибутов доступа.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где происходит работа пользователей.

Ключи от серверного помещения хранятся у администратора информационной безопасности и системного администратора ИСПДн. Уборка и регламентные работы в серверном помещении осуществляются под контролем системного администратора или администратора информационной безопасности.

В ИСПДн действует парольная политика, определены требования по хранению паролей и личных идентификаторов.

Вероятность реализации угрозы – ***низкая вероятность***.

Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ.

Защищаемая информация обрабатывается и хранится только на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора и администратора информационной безопасности.

Вероятность реализации угрозы **– *низкая вероятность*.**

Несанкционированное (в т.ч. непреднамеренное) отключение средств защиты.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены средства защиты ИСПДн.

В помещениях ИСПДн, установлена охранно-пожарная сигнализация, подключенная к пульту __01_____. В серверном помещении есть окона, установлена деревянная дверь, доступ разрешен только ограниченному кругу лиц. Бесконтрольное пребывание посторонних лиц в здании не допускается. Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора или администратора информационной безопасности.

В зданиях органов государственной власти организован пропускной режим. Доступ посторонних лиц в помещения, в которых производится обработка ПДн, ограничен.

Доступ к изменению настроек средств защиты информации, установленных на серверах ИСПДн, имеется только у администратора информационной безопасности ИСПДн.

Защищаемая информация обрабатывается и хранится только на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

При подключении пользователей к серверу ИСПДн создается защищенное соединение с помощью криптопровайдера _____ (или иные аналогичные сертифицированные средства защиты информации). При отключении криптопровайдера _____ на рабочей станции пользователя происходит разрыв соединения и отключение пользователя от сервера ИСПДн.

Вероятность реализации угрозы – ***низкая вероятность***.

Утрата ключей и атрибутов доступа.

Угроза может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Пользователи проходят обучение до начала работы в ИСПДн, а также несут административную ответственность за нарушение правил работы с ИСПДн.

В ИСПДн действует парольная политика, определены требования по хранению паролей и личных идентификаторов.

Вероятность реализации угрозы – ***низкая вероятность***.

Непреднамеренная модификация (уничтожение) информации сотрудником.

Угроза может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают правила работы с конфиденциальной информацией.

Периодически производится резервное копирование базы данных ИСПДн.

Пользователи проходят обучение до начала работы с приложением, а также несут административную ответственность за нарушение правил работы с ИСПДн.

Вероятность реализации угрозы – ***средняя вероятность***.

Разглашение информации сотрудниками, допущенными к ее обработке.

Угроза может осуществляться за счет действий пользователей ИСПДн, которые нарушают соглашение о конфиденциальности и неразглашении информации, обрабатываемой информации или не осведомлены о нем.

Пользователи несут административную ответственность за нарушение правил работы с ИСПДн и разглашение персональных данных.

Вероятность реализации угрозы – ***средняя вероятность***.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств:

Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой, загрузка с внешних носителей

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

Доступ посторонних лиц в помещения, в которых производится обработка ПДН, ограничен. Доступ в серверное помещение ЦОДа разрешен только ограниченному кругу лиц. Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора и администратора информационной безопасности.

Доступ пользователей к ПДн осуществляется с использованием технологии удаленного доступа, при этом защищаемая информация обрабатывается и хранится на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД с применением стандартных функций операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены средства защиты ИСПДн. При получении доступа в операционную среду, нарушитель может воспользоваться как стандартными функциями ОС или какой-либо прикладной программы общего пользования (например, СУБД), так и специально созданными для выполнения НСД программами, например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым словам и копирования;
- специальными программами просмотра и копирования записей в базах данных;

- программами быстрого просмотра графических файлов, их редактирования и копирования;
- программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.

Доступ посторонних лиц в помещения, в которых производится обработка ПДН, ограничен.

Пользователям запрещено самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПЭВМ или устанавливать дополнительно любые программные и аппаратные средства.

На серверах ИСПДн установлена сертифицированное _____.

Доступ пользователей к серверам ИСПДн осуществляется с использованием технологии удаленного доступа, при этом защищаемая информация обрабатывается и хранится на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

Вероятность реализации угрозы **– *низкая вероятность*.**

Угрозы НСД в виртуальной среде:

Некорректная настройка параметров гипервизора и виртуальных машин, влияющих на безопасность

Угроза осуществляется лицом, осуществляющим администрирование виртуальной среды.

При реализации данной угрозы происходит несанкционированный доступ (удаленный доступ из реальной среды или доступ в рамках виртуальной среды) к ресурсам виртуальных машин вследствие некорректных настроек гипервизора.

В ИСПДн применяется только лицензионное ПО платформы виртуализации _____. Настройка параметров гипервизора и виртуальных машин осуществляется с использованием штатной технической документации на ПО платформы виртуализации.

Вероятность реализации угрозы **– *низкая вероятность*.**

Ошибки в работе ПО гипервизора

Угроза может осуществляться со стороны лица, осуществляющего администрирование виртуальной среды, а также пользователями, имеющими легитимный доступ к определенной виртуальной машине, вследствие программных ошибок (закладок) в ПО гипервизора.

В ИСПДн применяется только лицензионное ПО платформы виртуализации _____.

Вероятность реализации угрозы **– *низкая вероятность*.**

Подмена исполняемых модулей ПО гипервизора

Угроза может осуществляться со стороны лица, осуществляющего администрирование виртуальной среды.

При реализации данной угрозы происходит несанкционированный доступ (удаленный доступ из реальной среды или доступ в рамках виртуальной среды) к ресурсам виртуальных машин вследствие искажения работы ПО гипервизора. В результате происходит несанкционированный доступ к хранимым, обрабатываемым и передаваемым между виртуальными машинами ПДн, а также нарушение доступности ИСПДн, развернутых в виртуальной среде.

Для защиты виртуальной инфраструктуры в ИСПДн применяется сертифицированное СЗИ _____. Настройку данного СЗИ производили сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Несанкционированный удаленный доступ к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера» на открытые сетевые порты сервера с гипервизором в случае возникновения в его ПО уязвимостей

Угроза осуществляется пользователем, имеющим сетевой доступ к сетевому сегменту, к которому подключен сервер с установленным гипервизором, а также внешний нарушитель, действующий из-за пределов сети, удаленно проникший в сетевой сегмент, к которому подключен сервер с установленным гипервизором. В результате происходит получение контроля над сервером с установленным гипервизором с полномочиями взломанной службы.

Системным администратором производится своевременная установка обновлений безопасности ПО гипервизора. На серверах установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Истощение вычислительных ресурсов сервера с гипервизором вследствие атак типа «отказ в обслуживании» в отношении виртуальных машин

Угроза осуществляется пользователями, имеющими доступ к сетевому сегменту, к которому подключен сервер с установленным гипервизором.

Результатом выполнения атак типа «отказ в обслуживании» является замедление работы или прекращение работы сервера с гипервизором вследствие истощения вычислительных ресурсов.

На серверах установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

С использованием штатных средств ПО гипервизора производится мониторинг загрузки мощностей серверов с гипервизорами.

Вероятность реализации угрозы **– *низкая вероятность*.**

Случайное или умышленное искажение/уничтожение образов виртуальных машин

Угроза может осуществляться со стороны лица, осуществляющего администрирование виртуальной среды.

В результате реализации угрозы происходит стирание образов или искажение образов штатными средствами виртуальной среды.

В ИСПДн производится периодическое резервное копирование образов виртуальных машин.

Вероятность реализации угрозы **– *низкая вероятность*.**

Получение несанкционированного доступа к консоли управления виртуальной инфраструктурой

Угроза осуществляется внутренними и внешними нарушителями, получившими несанкционированный доступ к консоли управления виртуальной инфраструктурой.

В результате реализации угрозы возможно несанкционированное изменение настроек виртуальной среды, приводящее к снижению уровня безопасности виртуальной среды, кража образов дисков виртуальных машин, несанкционированное изменение настроек виртуальной среды, приводящее к нарушению функционирования, разрушению виртуальной среды и краже обрабатываемых в ней ПДн.

В серверном помещении нет окон, установлена металлическая дверь, доступ разрешен только ограниченному кругу лиц. Бесконтрольное пребывание посторонних лиц в здании не допускается. Доступ к серверам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора и администратора информационной безопасности.

Для защиты виртуальной инфраструктуры в ИСПДн применяется сертифицированное СЗИ _____. Настройку данного СЗИ производили сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Получение несанкционированного доступа к настройкам виртуальных машин

Угрозу может осуществлять лицо, имеющее право доступа к консоли администрирования, но не имеющее права настройки определенных виртуальных машин.

В результате происходит несанкционированное изменение настроек виртуальной среды, приводящее к нарушению функционирования, разрушению виртуальной среды и краже обрабатываемых в ней ПДн.

Разграничение доступа по администрированию виртуальной среды производится с помощью сертифицированного СЗИ _____. Настройку данного СЗИ производили сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Подмена и/или перехват данных и оперативной памяти виртуальных машин в процессе их миграции средствами виртуальной среды

Угроза осуществляется пользователем, имеющим сетевой доступ к сегменту в котором происходит выполнение процедур миграции.

В результате происходит перехват сетевого трафика или вклинивание в сетевую сессию, в рамках которой выполняется миграция виртуальной машины (реализация атаки типа «человек посередине»). Происходит нарушение работоспособности мигрировавшей виртуальной машины, кража образа виртуальной машины и утечка обрабатываемых на ней данных.

Для защиты виртуальной инфраструктуры в ИСПДн применяется сертифицированное СЗИ _____. Настройку данного СЗИ производили сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Проведение сетевых атак между виртуальными машинами

Потенциальными нарушителями являются пользователи виртуальной инфраструктуры, а также внешний нарушитель, получивший доступ к сетевому сегменту с размещенными виртуальными машинами.

В результате реализации угрозы возможно выполнение атак типа «переполнение буфера», SQL-injection и пр. с использованием системных и прикладных уязвимостей.

Для защиты виртуальной инфраструктуры в ИСПДн применяется сертифицированное СЗИ _____. Настройку данного СЗИ производили сотрудники организации – лицензиата ФСТЭК.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____.

Вероятность реализации угрозы **– *низкая вероятность*.**

Получение несанкционированного доступа (удаленного) к управляющим интерфейсам компонент системы хранения данных

Угроза осуществляется путем НСД внешними и внутренними нарушителями, получившими доступ к сегменту сети с управляющими интерфейсами системы хранения данных.

В результате возможно уничтожение, искажение или несанкционированное копирование разделов системы хранения штатными средствами, а также нарушение работоспособности компонент системы хранения.

В ИСПДн производится периодическое резервное копирование образов виртуальных машин.

Система хранения данных в ИСПДн подключена напрямую к гипервизору, подключений к внешней сети не имеет.

Вероятность реализации угрозы **– *низкая вероятность*.**

Размещение информации различного уровня конфиденциальности в рамках единой аппаратной платформы

Угроза осуществляется легальным пользователем виртуальной машины с низким уровнем конфиденциальности.

В результате реализации угрозы возможно проведение сетевых атак из области виртуальных машин с низким уровнем конфиденциальности в отношении виртуальных машин с более высоким уровнем конфиденциальности.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Подключение к ИСПДн стороннего оборудования (компьютеров, внешних носителей и иных устройств, в том числе имеющих выход в беспроводные сети связи)

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн.

Защищаемая информация обрабатывается и хранится на серверах, на рабочих станциях пользователей происходит только отображение информации, без ее хранения.

Подключение внешних устройств и носителей информации к серверам ИСПДн разрешено только системному администратору и администратору информационной безопасности. Доступ посторонних лиц в серверное помещение ЦОД ограничен.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза внедрения вредоносных программ (вирусов).

Предпосылками, влияющими на возникновение данной угрозы могут быть бесконтрольное использование внешних носителей, а также наличие подключения к сетям связи общего пользования и международного обмена.

На всех рабочих станциях, входящих в состав ИСПДн, применяются антивирусные средства. На серверах ИСПДн установлен сертифицированный антивирус _____. Периодически производится обновление сигнатур вирусных баз. Управление антивирусной защитой серверов осуществляется централизованно.

Вероятность реализации угрозы – ***низкая вероятность***.

Недекларированные возможности системного ПО и ПО для обработки персональных данных.

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

На рабочих станциях и серверах ИСПДн устанавливается только лицензионное прикладное и системное ПО. Настройку и сопровождение приложений осуществляет сотрудник информационных технологий и документальной связи

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы НСД в ИСПДн, реализуемые по локальной сети:

Угроза «Анализ сетевого трафика» в локальной сети.

Эта угроза реализуется со стороны внутреннего нарушителя, по локальной сети, с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

Доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Угроза «Сканирование сети» в локальной сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей. Реализация данной угрозы в локальной сети наиболее вероятна со стороны внутреннего нарушителя.

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы **– *низкая вероятность*.**

Угроза выявления паролей внутри сети.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing).

Доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза удаленного запуска приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности,

целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

На серверах, входящих в состав ИСПДн установлен сертифицированный антивирус _____. Периодически производится обновление сигнатур вирусных баз.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы внедрения по сети вредоносных программ.

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

На всех рабочих станциях, входящих в состав ИСПДн, применяются антивирусные средства. На серверах, входящих в состав ИСПДн установлен сертифицированный антивирус _____. Периодически производится обновление сигнатур вирусных баз.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы НСД в ИСПДн, реализуемые с использованием протоколов межсетевого взаимодействия:

Угроза «Анализ сетевого трафика» при межсетевом взаимодействии

Доступ к ПДн осуществляется с использованием технологии удаленного доступа, при этом все ПДн обрабатываются только на сервере.

Доступ удаленных пользователей к персональным данным осуществляется по сети Интернет с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы **–** ***низкая вероятность***.

Угроза «Сканирование сети» при межсетевом взаимодействии

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Для защиты периметра сети ЦОД применяется сертифицированный межсетевой экран _____.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза подмены доверенного объекта при межсетевом взаимодействии

Доступ удаленных пользователей к персональным данным осуществляется по сети Интернет с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных во внешних сетях

Доступ удаленных пользователей к персональным данным осуществляется по сети Интернет с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза выявления паролей при межсетевом взаимодействии

Доступ удаленных пользователей к персональным данным осуществляется по сети Интернет с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угроза удаленного запуска приложений при межсетевом взаимодействии

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

На серверах ИСПДн установлен сертифицированный антивирус _____. Периодически производится обновление сигнатур вирусных баз. Пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы внедрения по сети вредоносных программ при межсетевом взаимодействии

На серверах ИСПДн установлен сертифицированный антивирус _____. Периодически производится обновление сигнатур вирусных баз. Пользователи проинструктированы о мерах предотвращения вирусного заражения.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы типа «Отказ в обслуживании».

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-

адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На серверах ИСПДн установлен сертифицированный межсетевой экран _____, настройку которого выполняли сотрудники организации – лицензиата ФСТЭК.

Для защиты периметра сети ЦОД применяется сертифицированный межсетевой экран _____.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы возникающие при передаче данных по каналам связи:

Угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств, с целью нарушения безопасности защищаемых средствами криптографической защиты информации (далее - СКЗИ) персональных данных или создания условий для этого (далее - атака) при нахождении в пределах контролируемой зоны

Для нейтрализации данной угрозы:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно- пропускным режимом;

- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;

- сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;

- пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

- утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;

- осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн;

- осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа;

- используются сертифицированные средства антивирусной защиты.

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы проведения атаки на этапе эксплуатации средств криптографической информации на следующие объекты:

А) документацию на СКЗИ и компоненты среды функционирования (далее - СФ) СКЗИ;

Б) 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;

Для нейтрализации данной угрозы:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно- пропускным режимом; документация на СКЗИ хранится у

ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения.

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

Для нейтрализации данной угрозы:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом;

- сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников;

- сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы использования штатных средств информационных систем персональных данных, ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий

Для нейтрализации данной угрозы:

-проводятся работы по подбору персоналов;

- помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

- сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

- осуществляется регистрация и учет действий пользователей;

- в ИСПДн используются:

- сертифицированные средства защиты информации от несанкционированного доступа;

- сертифицированные средства антивирусной защиты

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ

Для нейтрализации данной угрозы:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно- пропускным режимом;

- помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода.

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером

_____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий

Для нейтрализации данной угрозы:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно- пропускным режимом;

- помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации.

- доступ пользователей к персональным данным осуществляется с использованием технологии удаленного доступа, защищаемая информация передается по каналам связи общего пользования с использованием защищенного соединения по протоколу SSL. Обеспечение конфиденциальности и контроля целостности передаваемой информации реализовано посредством ее шифрования и имитозащиты криптопровайдером _____ (или иные аналогичные сертифицированные средства защиты информации), в соответствии с ГОСТ 28147-89, ГОСТ Р 34.10-2012.

Вероятность реализации угрозы – ***низкая вероятность***.

6.4. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПДН

Коэффициент реализуемости угрозы Y будет определяется соотношением

$$Y=(Y_1+Y_2)/2,$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \le Y \le 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \le 0,6$, то возможность реализации угрозы признается средней;

если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признается высокой;

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Отнесение угроз к актуальным производится по таблице 1.

Таблица 1.Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности ПДн представлена в таблице 2.

Таблица 2. Определение актуальных угроз

Наименование угрозы	Коэффициент вероятности реализации угрозы (Y_2)	Коэффициент реализуемости угрозы Y=(Y1+Y2)/20	Опасность угрозы	Актуальность угрозы
УГРОЗЫ УТЕЧКИ ПО ТЕХНИЧЕСКОМУ КАНАЛУ				
Угрозы утечки акустической информации				
Угрозы утечки акустической (речевой) информации	0 (маловероятно)	0,5 (средняя)	низкая	неактуально
Угрозы утечки видовой информации				
Просмотр информации на дисплее и других средствах отображения информации сотрудниками предприятия, не допущенными к персональным данным	5 (средняя вероятность)	0,75 (высокая)	низкая	актуально
Просмотр информации на экране монитора и принтера, посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Просмотр информации на дисплее и других средствах отображения информации, лицами, находящимися за пределами помещения в котором	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально

ведется обработка персональных данных				
Просмотр информации с помощью специальных электронных устройств съема, внедренных в служебных помещениях, или скрытно используемых физическими лицами при посещении ими служебных помещений	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы утечки информации по каналам ПЭМИН				
Побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы (КЗ)	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Утечка информации по сетям электропитания (за счет неравномерного потребления тока)	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств ИСПДн, или при наличии паразитной генерации в узлах (элементах) технических средств	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Радиоизлучения, формируемые в результате высокочастотного облучения технических средств ИСПДн, в которых проводится обработка информативных сигналов	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ				
Угрозы НСД в ИСПДн путем физического доступа				
Кража ПЭВМ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Кража носителей информации, в т.ч. содержащих образы виртуальных машин	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Кража ключей и атрибутов доступа	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Несанкционированное отключение средств защиты	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Утрата ключей и атрибутов	2	0,6	низкая	неактуально

доступа	(низкая вероятность)	(средняя)		
Непреднамеренная модификация (уничтожение) информации сотрудником.	5 (средняя вероятность)	0,75 (высокая)	низкая	актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5 (средняя вероятность)	0,75 (высокая)	средняя	актуально
Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой, загрузка с внешних носителей	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД с применением стандартных функций операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Подключение к ИСПДн стороннего оборудования (компьютеров, внешних носителей и иных устройств, в том числе имеющих выход в беспроводные сети связи)	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угроза внедрения вредоносных программ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Недекларированные возможности системного ПО и ПО для обработки ПДн	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы НСД в виртуальной среде				
Некорректная настройка параметров гипервизора и виртуальных машин, влияющих на безопасность	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Ошибки в работе ПО гипервизора	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Подмена исполняемых модулей ПО гипервизора	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Несанкционированный удаленный доступ к ресурсам гипервизора вследствие сетевых атак типа «переполнение буфера» на открытые сетевые порты сервера с гипервизором в случае возникновения в его ПО уязвимостей	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Истощение вычислительных ресурсов сервера с гипервизором	2 (низкая	0,6 (средняя)	низкая	неактуально

вследствие атак типа «отказ в обслуживании» в отношении виртуальных машин	вероятность)			
Случайное или умышленное искажение/уничтожение образов виртуальных машин	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Получение несанкционированного доступа к консоли управления виртуальной инфраструктурой	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Получение несанкционированного доступа к настройкам виртуальных машин	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Подмена и/или перехват данных и оперативной памяти виртуальных машин в процессе их миграции средствами виртуальной среды	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Проведение сетевых атак между виртуальными машинами	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Получение несанкционированного доступа (удаленного) к управляющим интерфейсам компонент системы хранения данных	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Размещение информации различного уровня конфиденциальности в рамках единой аппаратной платформы	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы НСД в ИСПДн, реализуемые по локальной сети				
Угроза «Сканирование сети» в локальной сети	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угроза «Анализ сетевого трафика» с перехватом переда-ваемой по локальной сети информации	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы выявления паролей внутри сети	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы удаленного запуска приложений	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы внедрения по сети вредоносных программ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы НСД в ИСПДн, реализуемые с использованием протоколов межсетевого взаимодействия				
Угрозы «Анализа сетевого трафика» при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угроза «Сканирование сети» при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы подмены доверенного объекта при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных во внешних сетях	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально

Угрозы выявления паролей при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы удаленного запуска приложений при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы внедрения вредоносных программ при межсетевом взаимодействии	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы возникающие при передаче данных по каналам связи				
Угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств, с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее - атака) при нахождении в пределах контролируемой зоны	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы проведения атаки на этапе эксплуатации средств криптографической информации на следующие объекты	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы получения в рамках предоставленных полномочий, а также в результате наблюдений следующей информации	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы использования штатных средств информационных систем персональных данных, ограниченного мерами, реализованными в информационной системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы физического доступа к СВТ, на которых реализованы СКЗИ и СФ	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально
Угрозы возможностей воздействия на аппаратные компоненты СКЗИ и СФ, ограниченных мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	2 (низкая вероятность)	0,6 (средняя)	низкая	неактуально

7. ЗАКЛЮЧЕНИЕ

С учётом анализа угроз, актуальными угрозами безопасности в _____ являются:

- Просмотр информации на дисплее и других средствах отображения информации сотрудниками предприятия, не допущенными к персональным данным;
- Непреднамеренная модификация (уничтожение) информации сотрудником, допущенными к ее обработке;
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

В соответствии с постановлением Правительства № 1119 от 01.11.2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах», исходя из анализа угроз безопасности ПДн, учитывая параметры и основные характеристики ИСПДн, применяемые технические и организационные меры обеспечения безопасности ПДн, а также с учётом последствия реализации угроз для субъектов ПДн можно классифицировать школу как информационную систему **второго класса защищенности (К2)** и как информационную систему персональных данных с необходимостью обеспечения **2-го уровня защищенности персональных данных (УЗ 2)**.

В Модели нарушителя определен наивысший тип нарушителя – $\mathbf{H_2}$.

Для защиты от нарушителя криптографическое средство должно обеспечить криптографическую защиту по уровню **КС2**.