Министерство образования Оренбургской области

Государственное автономное профессиональное образовательное учреждение
«Соль-Илецкий индустриально-технологический техникум» Оренбургской области

УТВЕРЖДАЮ:
Директор ГАПОУ «С-И ИТТ»
С.Н. Жидовинов
«10» января 2020 г.

ПОЛОЖЕНИЕ
модель угроз защиты персональных данных при обработке в информационной системе ГАПОУ «С-И ИТТ»

Соль-Илецк, 2020 г.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИИ

ИСПДн	Информационная система персональных данных обмена инфор
АРМ	мацией с ИСПДн центра обработки данных ФГБУ ФЦТ
ИБ	Автоматизированное рабочее место Информационная
ИР	безопасность Информационный ресурс
ИСПДн	Информационная система персональных данных Контролируемая
КЗ	зона
НЖМД	Накопитель на жестких магнитных дисках Несанкционированный
НСД	доступ Операционная система Персональные данные
ОС	Программное обеспечение Среда функционирования
ПДн	Персональная электронно-вычислительная машина Побочные
ПО	электромагнитные излучения и наводки Средства вычислительной
СФ	техники Система защиты информации Средство защиты
ПЭВМ	информации Средство криптографической защиты информации
ПЭМИН	Технические каналы утечки информации Технические средства
СВТ	Угрозы безопасности персональных данных Федеральная служба
СЗИ	безопасности Российской Федерации Федеральная служба по
СрЗИ	техническому и экспортному контролю Российской Федерации
СКЗИ	
ТКУИ	
ТС	
УБПДн ФСБ России	
ФСТЭК России	

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Атака	Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого
Аутентификационная информация	Информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)
Безопасность персональных данных	Состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных
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
Внешняя информационная система	Информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора
Внешняя информационно-телекоммуникационная сеть	Информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы
Доступ в информационную 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 её использования
Доступность информации	Свойство безопасности информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Защищенные линии связи	Линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность)
Идентификатор	Представление (строка символов), однозначно идентифици-

	рующее субъект и (или) объект доступа в информационной системе
Идентификация	Присвоение субъектам и объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Инцидент	Непредвиденное или не желательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)
Канал атаки	Среда переноса от субъекта к объекту атаки действий (а, возможно, и от объекта к субъекту атаки) осуществляемых при проведении атаки
Категория доступа к информации	Показатель, в зависимости от которого информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)
Компонент программного обеспечения	Составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию
Контролируемая зона	Пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств
Конфиденциальность информации	Свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право
Модель угроз	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации
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
Недекларированные возможности	Функциональные возможности ПО, 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

Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Отказ в обслуживании	Препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы
Периметр информационной системы	Физическая и (или) логическая граница информационной системы (сегмента информационной системы), в пределах которой оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации
Персональные данные	Любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных)
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	Лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования
Правила разграничения доступа	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Программная закладка	Код программы, преднамеренно внесённый в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и(или) блокировать аппаратные средства
Ресурс информационной системы	Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы
Роль	Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой
Событие безопасности (информационной)	Идентифицированное возникновение состояния информационной системы, сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

Субъект доступа	Пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа
Технические средства	Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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
Угрозы безопасности информации	Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе персональных данных
Уничтожение информации	Действия, в результате которых невозможно восстановить содержание информации в информационной системе персональных данных или в результате которых уничтожаются материальные носители информации
Управление доступом	Ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
Уязвимость	Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации
Целостность информации	Состояние информации, при котором её изменение осуществляется только преднамеренно субъектами, имеющими на него право

ВВЕДЕНИЕ

Настоящий документ (далее по тексту - Модель) описывает возможные угрозы безопасности персональным данным, которым подвержена информационная система персональных данных государственного автономного профессионального образовательного учреждения «Соль-Илецкий индустриально – технологический техникум» Оренбургской области (далее - Учреждение).

Данная Модель является частной и учитывает особенности информационной системы персональных данных государственного автономного профессионального образовательного учреждения «Соль-Илецкий индустриально – технологический техникум» Оренбургской области, используемые технические средства и технологические процессы обработки персональных данных (далее по тексту - ПДн), позволяет определить конкретные условия эксплуатации, защищаемые информационные ресурсы, совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведения атак, дать описания угроз безопасности персональным данным.

Разработка Модели велась на основании анализа исходных данных по объекту информатизации, законодательства Российской Федерации, нормативных и правовых документов органов исполнительной власти в области защиты персональных данных.

При разработке Модели применяется риск-ориентированный подход, при котором определяется перечень актуальных угроз безопасности персональным данным, и на их основе в дальнейшем разрабатывается система защиты информации (далее по тексту - СЗИ).

Средства защиты информационных ресурсов и технических средств ИСПДн, входящие в состав СЗИ, должны осуществлять защиту от влияния как преднамеренных, так и случайных событий, процессов или явлений, приводящих к несанкционированному доступу к персональным данным, а также возможности воздействия на компоненты ИСПДн, приводящие к сбою их функционирования и возникновению различных негативных последствий в отношении ресурсов СЗИ.

Модель разработана на основе методических документов ФСТЭК России и ФСБ России:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);
- «Состав и содержание 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» (утверждены приказом ФСБ России от 10 июля 2014 г. № 378);
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432);
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21).

Угрозы безопасности персональных данных (далее по тексту - УБПДн), содержащиеся в настоящей Модели, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн.

Для обеспечения актуальности Модели должен осуществляться ее плановый (регулярный) и внеплановый пересмотр.

Плановый пересмотр проводится в порядке проведения контроля состояния защиты информации (не реже одного раза в год).

Внеплановый пересмотр должен осуществляться в случаях:

- изменения требований законодательства Российской Федерации в области защиты информации, нормативно-правовых актов и методических документов, регулирующих защиту персональных данных;

- изменения конфигурации и условий размещения ИСПДн;
- изменения в составе основных элементов ИСПДн, которые могут повлиять на состав УБПДн.

1 ОПИСАНИЕ СИСТЕМЫ

1.1 Конфигурация ИСПДн ОИ ФЦТ

ИСПДн представляет собой информационную систему, объединяющую совокупность СВТ, являющихся частью IT-инфраструктуры Учреждения, и предназначенную для обработки персональных данных субъектов ПДн сотрудников оператора.

Технические средства, входящие в состав ИСПДн расположены по адресу: 461503, Оренбургская область, Соль-Илецкий район, г.Соль Илецк, ул. Орская, 169

Границей контролируемой зоны (КЗ) ИСПДн являются ограждающие конструкции помещений.

Параметры, оказывающие влияние на безопасность ПДн, приведены в таблице 1. Таблица 1 -

Параметры ИСПДн ОИ ФЦТ, оказывающие влияние на безопасность ПДн

Наименование параметра	Значение параметра
Тип информационной системы	ИСПДн, обрабатывающая иные категории ПДн
Принадлежность субъектов ПДн по отношению к оператору	Субъекты ПДн являются сотрудниками оператора
Количество субъектов ПДн	менее 100000

1.2 Структурные элементы ИСПДн

В состав ИСПДн входят следующие структурные элементы:

а) программно-технические средства обработки:
- общесистемное и специальное программное обеспечение, участвующее в обработке ПДн;
- средства и утилиты системы управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн;

б) средства защиты ПДн:

-средства управления доступом пользователей (встроенные в ОС);

-средства обеспечения регистрации и учета действий с информацией (встроенные в ОС);

-средства, обеспечивающие целостность данных (встроенные в ОС);

-средства антивирусной защиты;

в) каналы информационного обмена и телекоммуникации;

г) помещения, в которых размещены компоненты ИСПДн.

1.3 Состав и структура ПДн, обрабатываемых в ИСПДн

Состав обрабатываемых персональных данных в ИСПДн:

1. фамилия, имя, отчество;
2. дата рождения;
3. место рождения;
4. место фактического жительства;
5. место регистрации;
6. гражданство;
7. реквизиты документа, удостоверяющего личность (серия, номер, кем выдан, дата выдачи);
8. пол;
9. сведения о воинском учете;
10. реквизиты водительского удостоверения (при необходимости);
11. сведения о повышении квалификации и переподготовке;
12. сведения о имеющейся квалификационной категории;
13. сведения о семейном положении (состояние в браке);

14. наименование, номер, серия регистрационный номер и дата выдачи документа об образовании;
15. номер страхового свидетельства обязательного пенсионного страхования;
16. идентификационный номер налогоплательщика
17. номер страхового медицинского полиса обязательного медицинского страхования граждан;
18. номер телефона;
19. имеющиеся награды;
20. стаж работы;
21. адрес электронной почты;
22. доходы, полученные в данном учреждении

Также в ИСПДн циркулирует информация, не относящаяся к персональным данным, однако влияющая на целостность и устойчивость системы:

- управляющая информация (конфигурационные файлы, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), о системе управления ресурсами или средствах доступа к этим системам управления;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию об 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;
- служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия в результате обработки информации.

1.4 Режим обработки ПДн

Ввод данных в ИСПДн осуществляется сотрудниками Учреждения.

В ИСПДн производится обработка персональных данных субъектов ПДн, являющихся сотрудниками оператора. Состав ПДн указан в пп. 1.3.

Режим обработки предусматривает следующие действия с персональными данными: сбор, запись, систематизация, уточнение (обновление, изменение), передача.

В ИСПДн обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

2 СОВОКУПНОСТЬ ПРЕДПОЛОЖЕНИЙ О ВОЗМОЖНОСТЯХ, КОТОРЫЕ МОГУТ ИСПОЛЬЗОВАТЬСЯ ПРИ СОЗДАНИИ СПОСОБОВ, ПОДГОТОВКЕ И ПРОВЕДЕНИЯ АТАК

2.1 Описание нарушителей

С точки зрения наличия права постоянного или разового доступа в контролируемую зону объектов размещения ИСПДн все физические лица могут быть отнесены к двум категориям:

- категория I - лица, не имеющие права доступа в контролируемую зону ИСПДн;
- категория II - лица, имеющие право постоянного или разового доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

Внешними нарушителями могут быть как лица категории I, так и лица категории II. Внутренними нарушителями могут быть только лица категории II.

При описании нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа программного обеспечения (далее по тексту - ПО), средств защиты информации, включая СКЗИ не является целесообразным для нарушителей с учетом высокой стоимости разработки способов и средств атаки.

2.1.1 Внешние нарушители

Внешний нарушитель не имеет свободного доступа к системам и ресурсам ИСПДн, находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также через технические каналы утечки информации.

Нарушители данного вида при создании способов, подготовке и проведении атак могут использовать возможности из числа следующих:

- осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи;
- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой штатными средствами ИСПДн;
- проводить попытки навязывания ложной информации;
- проводить попытки внедрения вредоносного ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн;
- применять находящиеся в свободном доступе источники (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используются средства криптографической защиты информации. При этом может быть получена следующая информация:
- общие сведения об информационной системе (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
- сведения об информационных технологиях, базах данных, ТС (далее по тексту - ТС), ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, ТС, ПО, используемые в информационной системе совместно с СКЗИ;
- содержание конструкторской документации на СКЗИ;
- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ;
- общие сведения о защищаемой информации;
- сведения о каналах связи, по которым передаются персональные данные.

Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн.

Средства подготовки атаки, доступные данной категории нарушителя: доступные в свободной продаже технические средства и ПО, в том числе специально разработанное.

Данная категория нарушителей обладает только доступной из открытых источников информацией о применяемых в ИСПДн технических средствах.

Лица данной категории не являются доверенными.

2.1.2 Внутренние нарушители

К первой группе относятся сотрудники Учреждения, не являющиеся пользователями и не допущенные к ресурсам ИСПДн, но имеющие санкционированный или получившие разовый доступ в контролируемую зону (далее по тексту - КЗ). К этой категории нарушителей относятся технический и вспомогательный персонал: электрики, сантехники, уборщицы и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

При создании способов, подготовке и проведении атак нарушители данного типа могут использовать возможности из числа следующих:

- получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используются средства криптографической защиты информации. При этом может быть получена следующая информация:
- общие сведения об информационной системе (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
- сведения об информационных технологиях, базах данных, ТС (далее по тексту - ТС), ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, ТС, ПО, используемые в информационной системе совместно с СКЗИ;
- содержание конструкторской документации на СКЗИ;
- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ;
- общие сведения о защищаемой информации;
- сведения о каналах связи, по которым передаются персональные данные.

Средства атаки, доступные данной категории нарушителя: доступные в свободной продаже технические средства и ПО, в том числе специально разработанное.

Использование штатных средств ограничено мерами, реализованными в ИСПДн и направленными на предотвращение и пресечение несанкционированных действий.

Лица данной категории не являются доверенными, но нахождение лиц данной группы в помещениях с элементами ИСПДн, в силу принятых организационных мер возможно только под наблюдением ответственных лиц Учреждения, что делает невозможным проведение атаки. Поэтому лиц данной категории можно исключить из числа актуальных нарушителей ИБ ИСПДн.

Ко второй группе относятся зарегистрированные пользователи ИСПДн осуществляющие ограниченный доступ к защищаемой информации с рабочего места.

Лицо данной группы:

- обладает всеми возможностями лиц первой группы;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ИР ИСПДн;
- располагает ресурсами, к которым имеет доступ;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам ИСПДн;
- располагает сведениями о контролируемой зоне объекта, в которых размещены ресурсы ИСПДн;
- сведениями о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

Средства атаки, доступные данной категории нарушителя:

- доступные в свободной продаже ТС и ПО;
- штатные средства ИСПДн.

С учетом того, что СЗИ не может обеспечить ее защиту от действий, выполняемых в рамках предоставленных рассматриваемой группе нарушителей полномочий (например, защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации), и исходя

из анализа реализованных в ИСПДн административно-организационных мер безопасности в отношении персонала, допущенного для работы в ИСПДн, при построении модели нарушителя использовалось предположение о доверенности пользователей ИСПДн, которые имеют санкционированный доступ к защищаемой информации (персональным данным), доступ к ключевой информации, а также обладают знаниями о технологии обработки информации и системе принимаемых мер защиты.

Доверенность данной категории лиц означает, что они не являются злоумышленниками, т.е. не предпринимают умышленных действий (бездействия) при выполнении своих должностных обязанностей, могущих привести к реализации угроз безопасности информации. Поэтому в дальнейшем указанные лица не рассматриваются в качестве потенциальных нарушителей.

К третьей группе относятся зарегистрированные пользователи с полномочиями администратора ИСПДн, выполняющие обслуживание и поддержку эксплуатации ИСПДн, контроль за комплексом технических средств, ПО системы и СЗИ. К администраторам ИСПДн относятся следующие категории пользователей:

- сетевой администраторы;
- администратор безопасности.

Лицо данной группы:

- обладает всеми возможностями лиц второй группы;
- обладает полной информацией о системном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в ИСПДн;
- имеет доступ ко всем техническим средствам и данным ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств ИСПДн;
- располагает сведениями о контролируемой зоне объекта, в которых размещены ресурсы ИСПДн;
- сведениями о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.

Средства атаки, доступные данной категории нарушителя:

- штатные средства ИСПДн;
- доступные в свободной продаже ТС и ПО.

Лица данной категории обладают полными знаниями об ИСПДн.

Учитывая выполняемые функции, степень возложенной на них ответственности и высокий уровень их квалификации, лица, отнесенные к данной категории, проходят специальный отбор, в их отношении ведется непрерывный контроль. Лица данной категории выполняют все внутренние требования, регламенты и инструкции по обеспечению информационной, производственной и пожарной безопасности, регулярно проходят необходимый инструктаж.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить администраторов системы из числа актуальных нарушителей информационной безопасности (далее по тексту - ИБ) ИСПДн.

К четвертой группе относятся лица из числа программистов-разработчиков сторонних организаций, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

Средства атаки, доступные данной категории нарушителя:

- штатные средства;
- доступные в свободной продаже ТС и ПО, в том числе специально разработанные.

В отношении сотрудников сторонних организаций, привлекаемых к обслуживанию ИСПДн на основании договора, проводятся проверки по линии безопасности, благонадежность этих сотрудников подтверждается организацией-работодателем, в их отношении действуют документы, регламентирующие порядок обеспечения информационной безопасности и объектового режима. С компанией, привлекаемой к обслуживанию ИСПДн, заключается соглашение о конфиденциальности. Сотрудники сторонних организаций действуют на объекте расположения ИСПДн только в

сопровождении и под непрерывным контролем ответственных сотрудников Учреждения.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить лиц данной группы из числа актуальных нарушителей ИБ ИСПДн.

К пятой группе относится персонал сторонней организации, обеспечивающий поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, коммуникационном оборудовании, а также о средствах защиты информации, используемых в ИСПДн.

Средства атаки, доступные данной категории нарушителя:

- штатные средства;
- доступные в свободной продаже ТС и ПО, в том числе специально разработанные.

В отношении сотрудников сторонних организаций, привлекаемых к обслуживанию ТС ИСПДн на основании договора, также проводятся проверки по линии безопасности, благонадежность этих сотрудников подтверждается организацией-работодателем, в их отношении действуют документы, регламентирующие порядок обеспечения информационной безопасности и объектового режима. С компанией, привлекаемой к обслуживанию ТС ИСПДн, заключается соглашение о конфиденциальности. Сотрудники сторонних организаций действуют на объекте расположения АП ИСПДн только в сопровождении и под непрерывным контролем ответственных сотрудников Учреждения.

Исходя из комплекса приведенных факторов, полагаем целесообразным исключить лиц данной группы из числа актуальных нарушителей ИБ ИСПДн.

К шестой группе относятся лица, не являющиеся зарегистрированными пользователями системы, получившие разовый доступ в КЗ, в обязанности которых не входит обслуживание элементов ИСПДн. Как правило, лица данной категории являются сотрудниками сторонних организаций, приглашенными на площадку объекта в деловых целях.

Средства атаки, доступные данной категории нарушителя: доступные в свободной продаже ТС и ПО, в том числе специально разработанные.

Данная категория нарушителей обладает только доступной из открытых источников информацией о применяемых в ИСПДн технических средствах.

Лица данной категории не являются доверенными, но нахождение лиц данной группы на площадке объекта в силу принятых организационных мер возможно только под контролем ответственных лиц Учреждения. Поэтому лиц данной категории можно исключить из числа актуальных нарушителей ИБ ИСПДн.

2.2 Предположение о возможности сговора нарушителей

В данном разделе рассмотрены предположения о возможности и характере сговора нарушителей и о возможности преимуществ, которыми могут располагать нарушители, находящиеся в сговоре.

Возможность сговора внутренних нарушителей между собой практически не даёт преимуществ сговорившимся нарушителям, помимо тех, которыми они обладают по отдельности. Кроме того, ввиду принятых на объекте информатизации организационно-технических мер, вероятность сговора данных категорий лиц маловероятна.

Возможность сговора внутренних нарушителей с любыми внешними нарушителями, с одной стороны, практически не даёт преимуществ сговорившимся нарушителям перед внутренним нарушителем, имеющим право постоянного или разового доступа в КЗ, действующим в одиночку. С другой стороны ввиду принятых на объекте организационно-технических мер, повышает вероятность обнаружения их противоправных действий.

С учётом изложенного выше, можно сделать вывод о том, что сговор между внешними и внутренними нарушителями не предоставляет им никаких дополнительных возможностей по сравнению с внутренним нарушителем, организующим и проводящим атаки, пользуясь доступом в контролируемую зону.

Возможность сговора внешних нарушителей между собой не предоставляет им никаких дополнительных возможностей по нарушению безопасности информации в ИСПДн, помимо тех, которыми обладают по отдельности.

Таким образом, можно сделать вывод, что возможности нарушителей безопасности информации в ИСПДн, существенно ограничиваются принятыми на объекте информатизации организационно-техническими мерами по обеспечению порядка доступа в помещения, в которых размещены

технические средства обработки защищаемой информации ИСПДн, в том числе используемыми средствами защиты информации, а также необходимыми защитными мерами и устройствами, реализованными в оборудовании и программном обеспечении ИСПДн. Поэтому самостоятельно нарушители рассматриваемого типа могут осуществлять ограниченный набор действий, связанных с попытками доступа к информационным ресурсам ИСПДн.

2.3 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации: доступные в свободной продаже ТС и ПО, в том числе специально разработанные, а также программные и аппаратные компоненты криптосредств.

Внутренний нарушитель для доступа к защищаемой информации может использовать штатные средства ИСПДн. При этом его возможности по использованию перечисленных средств зависят от реализованных в ИСПДн организационно-технических мер.

2.4 Описание каналов атак

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- штатные программно-технические средства ИСПДн;
- коммутационное оборудование, расположенное в пределах контролируемой зоны, не защищенное от НСД к информации организационно-техническими мерами;
- электронные носители, в том числе съемные, сданные в ремонт и вышедшие из употребления; неучтенные носители информации;
- кабельные системы, расположенные, как в пределах контролируемой зоны, так и за ее пределами, не защищенные от НСД к информации организационно-техническими мерами.

2.5 Обобщенные возможности источников атак

На основании анализа исходных данных об ИСПДн, объектах защиты и источниках атак определены обобщенные возможности источников атак. Обобщенные возможности источников атак представлены в таблице 3.

Таблица 3 - Обобщенные возможности источников атак

№ п/п	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	нет

2.6 Обоснование неактуальности угроз

В таблице 4 приводятся организационно-технические меры, направленные на противодействие возможностям источников атак.

Таблица 4 - Возможности нарушителей и меры противодействия угрозам атак

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	не актуально	Проводятся работы по подбору персонала; Представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стой-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			ках), где расположены элементы ИСПДн, в том числе СКЗИ, и сотрудники, не являющиеся пользователями ИСПДн, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; 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 элементы ИСПДн, в том числе 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 элементы ИСПДн, в том числе СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; Утвержден перечень лиц, имеющих право доступа в помещения, где располагаются элементы ИСПДн, в том числе СКЗИ; Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; Осуществляется контроль целостности средств защиты; На АРМ (серверах), на которых установлены СКЗИ используются сертифицированные средства защиты информации от несанкционированного доступа; Используются сертифицированные средства антивирусной защиты.
1.2	Проведение атак на этапе эксплуатации СКЗИ на	не актуально	Проводятся работы по подбору персонала;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - элементы ИСПДн), на которых реализованы СКЗИ и СФ.		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.
1.3	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.	не актуально	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.
1.4	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Проводятся работы по подбору персоналов; Помещения, в которых располагаются элементы ИСПДн, 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 информа-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			ции; Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; В ИСПДн используются сертифицированные средства защиты информации от несанкционированного доступа; Сертифицированные средства антивирусной защиты.
2.1	Физический доступ к элементам ИСПДн, на которых реализованы СКЗИ и СФ.	не актуально	Проводятся работы по подбору персонала; Помещения, в которых располагаются элементы ИСПДн, 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.
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Проводятся работы по подбору персонала; 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 ответственных сотрудников Учреждения.
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; Высокая стоимость и сложность подготовки реализации возможности; Проводятся работы по подбору персонала; Доступ в контролируемую зону и помещения, где располагается элементы ИСПДн, на которых реализованы СКЗИ и СФ, обеспечивается в соответ-

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			ствии 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 ответственных сотрудников Учреждения; Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; Осуществляется регистрация и учет действий пользователей; На АРМ, на которых установлены СКЗИ используются сертифицированные средства защиты информации от несанкционированного доступа и сертифицированные средства антивирусной защиты.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; Высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с ис-	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; Высокая стоимость и сложность подготовки реализации возможности.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	пользованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.		
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; Высокая стоимость и сложность подготовки реализации возможности; 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 ответственных сотрудников Учреждения; Осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; Осуществляется регистрация и учет действий пользователей; На АРМ (серверах), на которых установлены СКЗИ используются сертифицированные средства защиты информации от несанкционированного доступа и сертифицированные средства антивирусной защиты.
4.2	Возможность располагать сведениями, содер-	не актуально	Не осуществляется обработка сведений, составляющих государственную

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	жащимися в конструкторской документации на аппаратные и программные компоненты СФ.		тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

2.7 Основные организационно-технические меры, необходимые для противодействия возможностям источников атак

Реализация угроз безопасности информации, обрабатываемых в информационных системах определяется возможностями источников атак. Для противодействия возможностями источников атак в Учреждении должны быть приняты следующие организационно-технические меры:

- на должности, в обязанности которых входят работа со средствами защиты, защищаемой информацией в том числе ПДн, назначаются ответственные добросовестные лица, имеющие положительные характеристики, ознакомленные с ответственностью за несоблюдение правил обеспечения безопасности информации, имеющие знания и навыки в работе со средствами вычислительной техники и защиты информации;
- определен порядок доступа в помещения с элементами ИСПДн и/или СКЗИ, лиц, не имеющих допуска к защищаемой информации;
- помещения, в которых располагаются элементы ИСПДн и/или СКЗИ, оснащены входными дверьми с замками;
- обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;
- утверждены правила доступа в помещения, где располагаются элементы ИСПДн и СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;
- назначены лица, отвечающие за администрирование информационной системы, безопасность информации и эксплуатацию СКЗИ;
- утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;
- документация на СКЗИ хранится у ответственного за СКЗИ в металлическом ящике;
- осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;
- осуществляется регистрация и учет действий пользователей с защищаемой информацией;
- осуществляется контроль целостности средств защиты;
- на элементах ИСПДн (АРМ), на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа и антивирусной защиты.

2.8 Определение класса, применяемого СКЗИ

Исходя из анализа данных, представленных в разделе 2 и при выполнении мер, изложенных в п.п 2.7, в соответствии с требованиями Приказа ФСБ России от 10.07.2014 № 378 для нейтрализации атак достаточно применение СКЗИ класса КС 1.

3 МОДЕЛЬ УГРОЗ

Модель угроз разрабатывается в соответствии с методологией ФСТЭК России, определённой в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года).

3.1 Идентификация уязвимых звеньев

Под уязвимым звеном подразумевается программное, аппаратное или программноаппаратное средство, включая средства защиты информации, а также носители информации, в т.ч. ПДн, в отношении которых возможна реализация угроз НСД или утечки по техническим каналам.

Согласно «Методике определения актуальных угроз персональных данных при их обработке в

информационных системах персональных данных» ФСТЭК России наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы.

Таким образом, идентификация уязвимых звеньев необходима для идентификации всех принципиально реализуемых в информационной системе угроз безопасности.

3.1.1 Идентификация технических каналов утечки информации

При обработке ПДн возможно возникновение следующих угроз утечки информации по ТКУИ:
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналам ПЭМИН.

Утечка акустической информации

Угроза утечки акустической (речевой) информации возможно при наличии функций голосового ввода защищаемой информации, в т.ч. ПДн, в ИСПДн или функций воспроизведения защищаемой информации, в т.ч. ПДн, акустическими средствами ИСПДн.

Утечка видовой информации

Реализация угрозы утечки видовой информации возможна за счет несанкционированного просмотра информации 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.

Утечка по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, технических средств, входящих в состав ИСПДн.

3.1.2 Идентификация уязвимых по отношению к НСД звеньев информационной системы

Несанкционированный доступ представляет собой второй способ реализации УБИ.

Уязвимые по отношению к НСД звенья представляют собой объекты среды информации на различных уровнях иерархии информационной инфраструктуры. Реализация угроз НСД осуществляется путём воздействия нарушителей на объекты среды информации с целью нарушения значимых характеристик ИБ системы.

Уязвимые по отношению к НСД звенья информационной системы представлены в таблице 5.

Таблица 5 - Уязвимые по отношению к НСД звенья информационной системы

Уровень иерархии информационной инфраструктуры	**Типы объектов среды (уязвимые звенья)**
Физический уровень	Линии связи внутри КЗ, линии связи вне контролируемой зоны, физические носители информации, включая НЖМД АРМ пользователей информационной системы
Сетевой уровень	Сетевое оборудование: маршрутизаторы, коммутаторы, межсетевые экраны, отделяющие информационную систему от сетей связи общего пользования
Уровень сетевых сервисов	Сетевые компоненты в составе информационной системы, сервисы терминального доступа, сервисы удалённого управления, другие служебные сервисы
Уровень ОС	Компоненты ОС, файлы, содержащие защищаемую информацию, в т.ч. ПДн
Уровень приложений	Прикладное ПО для доступа и обработки информации, в т.ч. ПДн

3.2 Возможные угрозы безопасности информации

3.2.1 *Угрозы утечки информации по техническим каналам*

В общем, при обработке информации возможно возникновение следующих угроз утечки информации по ТКУИ:

- угроза утечки акустической (речевой) информации;
- угроза утечки видовой информации;
- угроза утечки информации по каналам ПЭМИН.

Угроза утечки акустической информации возможна только в том случае, если в информационной системе предусмотрен голосовой ввод информации, в т.ч. ПДн, или предусмотрены функции воспроизведения информации, в т.ч. ПДн, акустическими средствами информационной системы.

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

Таким образом, реализация угрозы утечки акустической информации невозможна ввиду отсутствия источника угрозы.

Угрозы утечки видовой информации реализуются за счёт несанкционированного просмотра информации, в т.ч. ПДн, с экранов дисплеев и других средств отображения вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав информационной системы.

Экраны дисплеев рабочих мест пользователей расположены так, что визуальный просмотр информации исключен.

Таким образом, реализация угрозы утечки видовой информации признается маловероятной, а сама угроза считается неактуальной и далее не подлежит рассмотрению.

Для перехвата информации по каналам ПЭМИН нарушитель должен обладать дорогостоящей аппаратурой и иметь в своём составе специалистов высокой квалификации, достаточной для настройки аппаратуры, перехвата и выделения информативного сигнала. Кроме того, элементы ИСПДн экранируются несколькими несущими стенами, и информационный сигнал маскируется множеством паразитных сигналов элементов, не входящих в информационную систему.

Эти факторы позволяют сделать вывод, что вероятность наличия возможностей осуществить перехват ПЭМИН у кого-либо из нарушителей ИБ ничтожна мала.

Таким образом, реализация угрозы утечки по каналам ПЭМИН является маловероятной, а сама угроза считается неактуальной и далее не рассматривается.

3.2.2 Угрозы несанкционированного доступа к информации

Перечень возможных угроз НСД к информации в ИСПДн ОИ ФЦТ, факторов, приводящих к их возникновению и нарушаемых характеристик безопасности информации, обрабатываемой в ИСПДн, представлен в таблице 6.

Таблица 6 - Перечень возможных угроз безопасности информации в ИСПДн ОИ ФЦТ

Угроза безопасности информации	**Характеристика**	**Нарушаемая характеристика безопасности информации**
Угрозы уничтожения, хищения аппаратных средств информационной системы, носителей информации путём физического доступа к элементам информационной системы		
Кража СВТ	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы системы	Конфиденциальность
Кража носителей информации	Угроза осуществляется путём НСД внешними и внутренними нарушителями к носителям информации	Конфиденциальность
Кража ключей и атрибутов доступа	Угроза осуществляется путём НСД внешними и внутренними нарушителями к носителям информации	Конфиденциальность
Кража, модификация, уничтожение информации	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей	Конфиденциальность Целостность Доступность
Вывод из строя узлов СВТ, каналов связи	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи	Доступность
Несанкционированное отключение встроенных средств защиты	Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн	Конфиденциальность Целостность Доступность
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
Действия вредоносных программ (вирусов)	Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций: -скрывать признаки своего присутствия в программной среде компьютера; - обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти; разрушать (искажать произвольным образом) код программ в оперативной памяти; -выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме её выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.); -сохранять фрагменты информации из оперативной памяти в некоторых областях внешней	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	памяти прямого доступа (локальных или удалённых); -искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных	
Недекларированные возможности системного и прикладного ПО	Недекларированные возможности - функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации	Конфиденциальность Целостность Доступность
Установка ПО, не связанного с исполнением служебных обязанностей	Угроза осуществляется путём несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей системы или её элементов	Конфиденциальность Целостность Доступность
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн *и СЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера*		
Утрата ключей и атрибутов доступа	Угроза осуществляется за счёт действия человеческого фактора пользователей ИС, которые нарушают положения парольной политики в части их создания (создают лёгкие 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	Конфиденциальность Целостность Доступность
Непреднамеренная модификация (уничтожение) информации сотрудниками	Угроза осуществляется за счёт действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИС или не осведомлены о них	Целостность
Непреднамеренное отключение средств защиты	Угроза осуществляется за счёт действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них	Конфиденциальность Целостность Доступность
Выход из строя аппаратно-программных средств	Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации	Целостность Доступность
Сбой системы электроснабжения	Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации	Целостность Доступность

Угроза безопасности информации	**Характеристика**	**Нарушаемая характеристика безопасности информации**
Стихийное бедствие	Угроза осуществляется вследствие несоблюдения мер пожарной безопасности	Доступность
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Угроза осуществляется путём НСД внутренних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей	Конфиденциальность Целостность
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Угроза осуществляется за счёт действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них	Конфиденциальность
Угрозы несанкционированного доступа по каналам связи		
«Анализ сетевого трафика»: - перехват за пределами контролируемой зоны; - перехват в пределах контролируемой зоны внешними нарушителями; -перехват в пределах контролируемой зоны внутренними нарушителями.	Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль	Конфиденциальность Целостность Доступность
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	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.	Конфиденциальность Целостность Доступность
Угрозы выявления паролей	Цель реализации угрозы состоит в получении НСД путём 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 (IPspoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путём последовательного подбора паролей. В случае успеха злоумышленник может создать	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.	
У грозы получения НСД путём подмены доверенного объекта сети	Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к сети. Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения. Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.	Конфиденциальность Целостность Доступность
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 системы 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 (Pingflooding), шторм запросов на установление TCP- соединений (SYN-flooding), шторм запросов к сетевому устройству: явный отказ в обслуживании, вызванный исчерпанием ресурсов ИС 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 пе-	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	редачи, 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), (при наличии почтового сервера - шторм сообщений почтовому серверу (Spam)); - явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами системы при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, DNSflooding) 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 «PingDeath»), 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 удалённого доступа к информации в системе, передача с одного адреса такого количества запросов на подключение к техническому средству в составе системы, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечёт за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка системы из-за невозможности системы заниматься ничем другим, кроме обработки запросов.	
Угроза удалённого запуска приложений	Угроза заключается в стремлении запустить на хосте системы различные предварительно внедрённые вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль над работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых	Конфиденциальность Целостность Доступность

Угроза безопасности информации	Характеристика	Нарушаемая характеристика безопасности информации
	прикладной программой процессов и др. Выделяют три подкласса данных угроз: - распространение файлов, содержащих несанкционированный исполняемый код; - удалённый запуск приложения путём переполнения буфера приложений; -удалённый запуск приложения путём использования возможностей удалённого управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.	
У грозы 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.	Конфиденциальность Целостность Доступность

3.3 Определение актуальных угроз безопасности информации

Процесс выделения актуальных угроз из общего перечня угроз выполняется в соответствии с Методикой определения актуальных угроз ФСТЭК России.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность для защищаемой информации, в т.ч. ПДн. Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищённости и частота (вероятность) реализации рассматриваемой угрозы. Степень опасности каждой угрозы оценивается экспертным методом.

3.3.1 Определение уровня исходной защищённости ИСПДн

В данном разделе ИСПДн рассматривается в качестве объекта, в котором обрабатываются персональные данные (информационной системы персональных данных).

Под уровнем исходной защищённости информационной системы понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик. Для определения уровня исходной защищённости производится оценка этих характеристик по трём качественным показателям: «Высокий», «Средний» и «Низкий».

В соответствии с Методикой определения актуальных угроз, информационной системе присваивается высокий уровень исходной защищённости, если не менее 70% характеристик соответствуют уровню «Высокий», а остальные - уровню «Средний». «Средний» уровень исходной защищённости присваивается информационной системе в случае, если не менее 70% характеристик соответствуют уровню не ниже «Средний», а остальные - «Низкому» уровню.

При составлении перечня актуальных угроз безопасности информации каждой степени исходной защищённости (Y1) ставится в соответствие числовой коэффициент, а именно:

0 - для высокой степени исходной защищённости;

5 - для средней степени исходной защищённости;

10 - для низкой степени исходной защищённости.

Результаты определения показателей исходной защищённости для ИСПДн ОИ ФЦТ приведены в таблице 7.

Таблица 7 - Показатели исходной защищённости ИСПДн ОИ ФЦТ

Технические и эксплуатационные характеристики ИСПДн	Уровень защищённости		
	Высокий	Средний	Низкий

Технические и эксплуатационные характеристики ИСПДн	Уровень защищённости		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная ИСПДн, развёрнутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями пользования между сотрудниками бухгалтерии	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, сортировка, модификация, передача		+	
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определённые перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн		+	
5. По наличию соединений с другими базами иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			+
6. По уровню обезличивания ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объёму ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации	+		

Уровень «высокий» имеют 29% характеристик информационной системы, что меньше значения 70%. Уровень «не ниже средний» имеют 57% характеристик системы, что меньше значения 70%. Таким образом, исходная защищённость ИСПДн ОИ ФЦТ определяется как низкая и числовой коэффициент Y1 устанавливается равным десяти (Y1 = 10).

3.3.2 Вероятность реализации угроз безопасности информации

Под вероятностью реализации угрозы понимается определяемый экспертным путём показателя, характеризующий, насколько вероятным является реализация конкретной УБИ в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по четырём вербальным градациям этого показателя:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (Y2 = 2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны (Y2 = 5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности информации не приняты (Y2 = 10).

Оценка вероятности реализации угроз безопасности персональных данных в ИСПДн ОИ ФЦТ приведена ниже.

3.3.2.1 Угрозы несанкционированного доступа к информации

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

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

3.3.2.1.1 Угрозы уничтожения, хищения аппаратных средств информационной системы, носителей информации путём физического доступа к элементам информационной системы

Кража СВТ.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн ОИ ФЦТ оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Кража носителей информации.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн ОИ ФЦТ оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Кража ключей и атрибутов доступа.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн ОИ ФЦТ оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Кражи, модификации, уничтожения информации.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн ОИ ФЦТ оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Вывод из строя СВТ, каналов связи.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн ОИ ФЦТ оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Несанкционированное отключение встроенных средств защиты.

В Учреждении введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн оборудовано крепкими дверьми, в нерабочее время двери помещения закрываются на замок. Доступ к настройкам встроенных средств защиты информации предоставляется только администратору безопасности информации ИСПДн.

Вероятность реализации угрозы - маловероятно.

3.3.2.1.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)

Действия вредоносных программ (вирусов).

В Учреждении на АРМ пользователей ИСПДн сертифицированные ФСТЭК России средства антивирусной защиты не установлены.

Вероятность реализации угрозы - высокая.

Недекларированные возможности системного и прикладного ПО.

К использованию на АРМ пользователей ИСПДн допускается только лицензионное программное обеспечение. Получение обновлений программного обеспечения осуществляется из доверенных источников.

Вероятность реализации угрозы - низкая.

Установка ПО, не связанного с исполнением служебных обязанностей.

В системе не введено разграничение прав пользователей на установку ПО, пользователи не проинструктированы о политике установки ПО.

Вероятность реализации угрозы - высокая.

3.3.2.1.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера

Утрата ключей и атрибутов доступа.

В ИСПДн не введено ограничение прав пользователей на смену паролей, пользователи не проинструктированы о парольной политике.

Вероятность реализации угрозы - высокая.

Непреднамеренная модификация (уничтожение) информации сотрудниками.

Все пользователи проходят обязательный инструктаж о правилах работы в ИСПДн (ознакомление с правилами работы различных приложений, необходимых для функционирования системы).

Вероятность реализации угрозы - низкая.

Непреднамеренное отключение средств защиты.

В организации введён контроль доступа в контролируемую зону, все пользователи проходят обязательный инструктаж о правилах работы в ИСПДн.

Вероятность реализации угрозы - маловероятно.

Сбой системы электроснабжения.

В ИСПДн ко всем ключевым элементам ИС источники бесперебойного питания не подключены.

Вероятность реализации угрозы - высокая.

Стихийное бедствие.

Все элементы ИСПДн расположены в помещении, оснащённом пожарной сигнализацией, пользователи проинструктированы о действиях в случае возникновения нештатных ситуаций.

Вероятность реализации угрозы - маловероятно.

3.3.2.1.4 Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лицами, не допущенными к её обработке.

В организации введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн оборудовано датчиками охранной сигнализации, в нерабочее время двери закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке.

Пользователи ИСПДн осведомлены о порядке работы с защищаемой информацией, а также подписали соглашение о неразглашении.

Вероятность реализации угрозы - маловероятно.

3.3.2.1.5 Угрозы несанкционированного доступа по каналам связи

Угроза «Анализ сетевого трафика».

Угроза подразделяется на следующие виды:

Перехват за пределами контролируемой зоны.

В ИСПДн сертифицированные средства межсетевого экранирования и криптографической защиты не установлены.

Вероятность реализации угрозы - высокая.

Перехват в пределах контролируемой зоны внешними нарушителями.

В организации введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн оборудовано датчиками охранной сигнализации, в нерабочее время двери закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В организации введён контроль доступа в контролируемую зону, помещение с элементами ИСПДн оборудовано датчиками охранной сигнализации, в нерабочее время двери закрываются на замок.

Вероятность реализации угрозы - маловероятно.

Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.

В ИСПДн сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений не установлены.

Вероятность реализации угрозы - высокая.

Угроза выявления паролей.

В ИСПДн сертифицированные ФСТЭК России средства межсетевого экранирования, обнаружения вторжений и антивирусной защиты не установлены.

Вероятность реализации угрозы - высокая.

Угрозы получения НСД путём подмены доверенного объекта.

В ИСПДн сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений не установлены.

Вероятность реализации угрозы - высокая.

Угрозы внедрения по сети вредоносных программ.

В ИСПДн сертифицированные ФСТЭК России средства межсетевого экранирования и антивирусной защиты не установлены.

Вероятность реализации угрозы - высокая.

3.3.2.2 Реализуемость угроз безопасности информации

По итогам оценки уровня защищённости (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением

Y = (Y1 + Y2)/20.

Оценка реализуемости угроз представлена в таблице 8.

Таблица 8 - Реализуемость угроз безопасности информации

Тип угроз безопасности информации	Коэффициент реализуемости угрозы (Y)	Возможность реализации
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств информационной системы путём физического доступа к элементам ИСПДн		
Кража ПЭВМ	0,5	средняя
Кража носителей информации	0,5	средняя
Кража ключей и атрибутов доступа	0,5	средняя
Кражи, модификации, уничтожение информации	0,5	средняя
Вывод из строя СВТ, каналов связи	0,5	средняя
Несанкционированное отключение средств защиты	0,5	средняя
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
Действия вредоносных программ (вирусов)	1	очень высокая
Недекларированные возможности системного и прикладного ПО	0,6	средняя
Установка ПО, не связанного с исполнением служебных обязанностей	1	очень высокая

Тип угроз безопасности информации	Коэффициент реализуемости угрозы (Y)	Возможность реализации
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн *и СрЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера*		
Утрата ключей и атрибутов доступа	1	очень высокая
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,6	средняя
Непреднамеренное отключение средств защиты	0,5	средняя
Сбой системы электроснабжения	1	очень высокая
Стихийное бедствие	0,5	средняя
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лицами, не допущенных к её обработке	0,5	средняя
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	0,5	средняя
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн *и принимаемой из внешних сетей информации:*		
Перехват за переделами контролируемой зоны	1	очень высокая
Перехват в пределах контролируемой зоны внешними нарушителями	0,5	средняя
Перехват в пределах контролируемой зоны внутренними нарушителями	0,5	средняя
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	1	очень высокая
Угрозы выявления паролей	1	очень высокая
Угроза получения НСД путём подмены доверенного объекта	1	очень высокая
Угрозы типа «Отказ в обслуживании»	1	очень высокая
Угрозы удалённого запуска приложений	1	очень высокая
Угрозы внедрения по сети вредоносных программ	1	очень высокая

3.3.2.3 Определение опасности и актуальности угроз безопасности информации

При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определялся вербальный показатель опасности для узла информационной системы. 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.

Затем осуществляется выбор из перечня угроз безопасности тех, которые относятся к актуальным для данной информационной системы, в соответствии с правилами, представленными в таблице 9.

Таблица 9 - Правила отнесения угрозы безопасности 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

Результаты оценки актуальности угроз для ИСПДн ОИ ФЦТ приведены в таблице 10.

Таблица 10 - Актуальные угрозы безопасности информации для ИСПДн ОИ ФЦТ

Тип угроз	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угрозы несанкционированного доступа к информации			
Угрозы уничтожения, хищения аппаратных средств информационной системы путем физического доступа к элементам информационной системы			
Кража СВТ	средняя	низкая	неактуальная
Кража носителей информации	средняя	низкая	неактуальная
Кража ключей и атрибутов доступа	средняя	низкая	неактуальная
Кражи, модификации, уничтожения информации	средняя	низкая	неактуальная
Вывод из строя СВТ, каналов связи	средняя	низкая	неактуальная
Несанкционированное отключение средств защиты	средняя	низкая	неактуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)			
Действия вредоносных программ (вирусов)	очень высокая	средняя	актуальная
Недекларированные возможности системного и прикладного ПО	средняя	низкая	неактуальная
Установка ПО, не связанного с исполнением служебных обязанностей	очень высокая	низкая	актуальная
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн *и СрЗИ в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера*			
Утрата ключей и атрибутов доступа	очень высокая	средняя	актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя	средняя	актуальная
Непреднамеренное отключение средств защиты	средняя	средняя	актуальная
Сбой системы электроснабжения	очень высокая	низкая	актуальная
Стихийное бедствие	средняя	низкая	неактуальная
Угрозы преднамеренных действий внутренних нарушителей			
Доступ к информации, модификация, уничтожение лицами, не допущенными к её об-	средняя	средняя	актуальная

Тип угроз	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
работке			
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке	средняя	средняя	актуальная
Угрозы несанкционированного доступа по каналам связи			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации:			
Перехват за пределами контролируемой зоны	очень высокая	низкая	актуальная
Перехват в пределах контролируемой зоны внешними нарушителями	средняя	низкая	неактуальная
Перехват в пределах контролируемой зоны внутренними нарушителями	средняя	низкая	неактуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	очень высокая	средняя	актуальная
Угрозы выявления паролей	очень высокая	средняя	актуальная
Угроза получения НСД путём подмены доверенного объекта	очень высокая	средняя	актуальная
Угрозы типа «Отказ в обслуживании»	очень высокая	низкая	актуальная
Угрозы удалённого запуска приложений	очень высокая	высокая	актуальная
Угрозы внедрения по сети вредоносных программ	очень высокая	низкая	актуальная

Таким образом, в результате анализа были выявлены следующие актуальные угрозы:

- действия вредоносных программ (вирусов);
- установка ПО, не связанного с исполнением служебных обязанностей;
- утрата ключей и атрибутов доступа;
- непреднамеренная модификация (уничтожение) информации сотрудниками;
- непреднамеренное отключение средств защиты;
- сбой системы электроснабжения;
- доступ к информации, модификация, уничтожение лицами, не допущенными к её обработке;
- разглашение информации, модификация, уничтожение сотрудниками, допущенными к её обработке;
- перехват за переделами контролируемой зоны;
- угрозы сканирования, направленные на выявление типа операционной системы элементов ИСПДн, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угроза получения НСД путём подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удалённого запуска приложений;
- угрозы внедрения по сети вредоносных программ.

4 ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДн

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» ИСПДн относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн, актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн, на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн, необходимо обеспечить 4-ый уровень защищенности ПДн.

5 СОСТАВ И СОДЕРЖАНИЕ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Выбор мер защиты информации осуществляется исходя из уровня защищенности ИСПДн, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности ПДн, включенных в модель угроз, а также с учетом структурно-функциональных характеристик ИСПДн, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в ИСПДн, а также иные характеристики системы, применяемые информационные технологии и особенности функционирования.

5.1 Базовый набор мер обеспечения безопасности ПДн

В соответствии с Приказом ФСТЭК России № 21 от «18» февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для установленного 4-ый уровня защищенности ПДн в ИСПДн необходимо обеспечение следующего базового набора мер обеспечения безопасности ПДн, приведенного в таблице 11.

Таблица 11 - Базовый набор мер обеспечения безопасности ПДн

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

V. Регистрация событий безопасности (РСБ)

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ. 7	Защита информации о событиях безопасности

VI. Антивирусная защита (АВЗ)

АВЗ.1	Реализация антивирусной защиты

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
Х[. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ХИ Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ХШ. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

5.2 Адаптация базового набора мер обеспечения безопасности ПДн

С учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе), а так же актуальных угроз безопасности персональных данных для ИСПДн ОИ ФЦТ необходимо принятие адаптированного набора мер защиты информации, приведенного в таблице 12.

Таблица 12 - Адаптированный набор мер обеспечения безопасности ПДн

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

V. Регистрация событий безопасности (РСБ)

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ. 7	Защита информации о событиях безопасности

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

5.3 Уточнение адаптированного базового набора мер защиты персональных данных

Уточнение адаптированного базового набора мер защиты персональных данных проводится с учетом результатов оценки возможности адаптированного базового набора мер по обеспечению безопасности персональных данных адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз, или снизить вероятность их реализации исходя из условий функционирования информационной системы.

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

Состав и содержание уточненного адаптированного базового набора мер защиты информации для ИСПДн приведены в таблице 13.

Таблица 13 - Уточненный адаптированный набор мер ПДн

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
I. Идентификация и аутентификация субъектов доступа к объектам доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

III. Ограничение программной среды (ОПС)

ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

IV. Защита машинных носителей персональных данных (ЗНИ)

ЗНИ.1	Учет машинных носителей персональных данных
ЗНИ.2	У правление доступом к машинным носителям персональных данных

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

V. Регистрация событий безопасности (РСБ)

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ. 7	Защита информации о событиях безопасности

VI. Антивирусная защита (АВЗ)

АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)

АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации

X Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

XИ Защита технических средств (ЗТС)

ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации,

Условное обозначение и номер меры	Меры обеспечения безопасности ПДн
	средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
XУ. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

5.4 Дополнение уточненного адаптированного базового набора мер защиты информации

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации», необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» для обеспечения 4-ый уровня защищенности ПДн, при их обработке в ИСПДн необходимо выполнение следующих требований:

- назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в ИСПДн;
- назначение ответственного за обеспечение функционирования и безопасности криптосредств;
- обучение лиц, использующих криптосредства, работе с ними;
- организация поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним;
- организация учета лиц, допущенных к работе с СКЗИ, предназначенных для обеспечения безопасности ПДн в ИСПДн;

-организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, в т.ч. оснащение помещений входными дверьми с замками, обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

- утверждение документа, определяющего перечень лиц, доступ которых к защищаемой информации, в т.ч. персональным данным, обрабатываемым в ИСПДн необходим для выполнения ими служебных (трудовых) обязанностей;

-утверждение правил доступа в помещения, в которых размещен ИСПДн в рабочее и нерабочее время, а также в нештатных ситуациях;

- утверждения перечня лиц, имеющих право доступа в помещения, в которых размещен ИСПДн;
- 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;
- организация учета машинных носителей ПДн;
- организация хранения съемных машинных носителей ПДн в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей. В случае если на съемном машинном носителе информации хранится только информация, в т.ч. персональные данные, в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6 РЕКОМЕНДУЕМЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для выполнения требований Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных», приказа ФСТЭК России № 21 от «18» февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других нормативных правовых актов в области защиты информации рекомендуется осуществить мероприятия по физической и программно-аппаратной защите, а также ряд мероприятий организационного характера.

Рекомендации по проведению мероприятий по защите персональных данных в ИСПДн приведены в таблице 14.

Таблица 14 - Мероприятия по защите персональных данных в ИСПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Использование сертифицированных ФСТЭК России СЗИ от НСД	
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Отображение символа «*» или «•» при вводе аутентификационной информации	
II. У правление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж администраторов информационной системы
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка матрицы доступа субъектов доступа к объектам доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования и штатных средств ОС	Разработка инструкций, инструктаж пользователей и администраторов системы
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, матрицы доступа
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования	Разработка инструкций, матрицы доступа
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж пользователей системы

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Использование сертифицированных ФСТЭК России СЗИ от НСД и штатных средств ОС	Разработка инструкций, инструктаж пользователей системы
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей информационной системы
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Использование сертифицированных средств межсетевого экранирования	
III. Ограничение программной среды (ОПС)			
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		Разработка инструкций, инструктаж пользователей и администраторов системы
IV. Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.1	Учет машинных носителей персональных данных		Разработка инструкций, инструктаж пользователей системы
ЗНИ.2	Управление доступом к машинным носителям персональных данных	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей и администраторов системы
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей и администраторов системы
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля, средств обнаружения вторжений, средств анализа защищен-	Разработка организационно-распорядительной документации по защите информации о событиях безопасности

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
		ности	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля, средств обнаружения вторжений, средств анализа защищенности	Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля, средств обнаружения вторжений, средств анализа защищенности	
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		Разработка организационно-распорядительной документации по защите информации о событиях безопасности
РСБ. 7	Защита информации о событиях безопасности	Использование сертифицированных ФСТЭК России СЗИ от НСД, средств межсетевого экранирования, средств антивирусного контроля, средств обнаружения вторжений	Разработка организационно-распорядительной документации по защите информации о событиях безопасности
VI. Антивирусная защита (АВ3)			
АВ3.1	Реализация антивирусной защиты	Использование средств антивирусной защиты, сертифицированных ФСТЭК России	Разработка инструкции по организации антивирусной защиты, проведение инструктажа пользователей
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Использование средств антивирусной защиты, сертифицированных ФСТЭК России	Инструктаж пользователей и администраторов информационной системы
VII. Контроль (анализ) защищенности персональных данных (АН3)			
АН3.2	Контроль установки обновлений программного обеспечения,		Разработка инструкций, инструктаж

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
	включая обновление программного обеспечения средств защиты информации		пользователей и администраторов информационной системы
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		Разработка организационно-распорядительной документации, регламентирующей проведение периодического контроля информационной системы, в т.ч. состава технических средств, программного обеспечения и средств защиты информации
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения средств защиты информации	Использование сертифицированных ФСТЭК России СЗИ от НСД	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	Резервное копирование	Разработка инструкций, инструктаж пользователей системы
XII. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования		Утверждение схемы границ контролируемой зоны информационной системы
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты ин-		Разработка организационно-распорядительной документации, обеспечивающей ограничение доступа посторонних лиц в пределах КЗ, ограничение доступа к средствам защиты информации, к техническим сред-

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн	Мероприятия по защите ПДн	
		Технические	Организационные
	формации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены		ства и средствам обеспечения функционирование информационной системы
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		Разработка инструкций, проведение инструктажа, ограничение доступа посторонних лиц в пределы КЗ
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны	Использование СКЗИ, сертифицированных ФСБ России	Разработка инструкций, инструктаж пользователей
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы персональных данных		Разработка инструкций, инструктаж пользователей
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Использование сертифицированных ФСТЭК России СЗИ от НСД	Разработка инструкций, инструктаж пользователей и администраторов информационной системы
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		Разработка инструкций, инструктаж пользователей и администраторов информационной системы

6.1 Организационные мероприятия

В рамках СЗИ ИСПДн рекомендуется реализовать следующие организационные меры защиты:

- назначить лицо (работник), ответственное за обеспечение безопасности персональных данных в ИСПДн;
- назначить лицо (работник), ответственное за защиту информации в ИСПДн;
- назначить ответственного за обеспечение функционирования и безопасности криптосредств;
- разработать документы, регламентирующие обработку персональных данных в ИСПДн;
- организовать разделение в ИСПДн функций по управлению (администрированию) ИСПДн, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций;

- организовать процедуры доступа работников в помещения с элементами ИСПДн, а также к техническим средствам, предназначенным для обработки защищаемой информации;

- организовать процедуры ознакомления работников, непосредственно осуществляющих обработку защищаемой информации, с требованиями законодательных и нормативных актов в области защиты информации;
- организовать инструктажи и процедуры повышения осведомленности работников, осуществляющих обработку защищаемой информации;
- организовать инструктаж лиц, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с ними;
- организовать процедуры контроля за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- организовать процедуры учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- установить правила разграничения доступа к информационным ресурсам ИСПДн;
- организовать правила антивирусной защиты информации;
- организовать учет лиц, допущенных к работе в ИСПДн;
- организовать учет машинных носителей персональных данных;
- организовать процедуры резервного копирования защищаемой информации;
- использовать для электропитания основных элементов ИСПДн источники бесперебойного питания (ИБП);
- организовать правила парольной защиты;
- организовать обучение лиц, использующих криптосредства, работе с ними;
- организовать поэкземплярный учет криптосредств, эксплуатационной и технической документации к ним;
- организовать учет лиц, допущенных к работе с СКЗИ, используемыми в ИСПДн;
- организовать процедуры проведения периодического внутреннего контроля и (или) аудита соответствия обработки информации требованиям законодательных и нормативных актов в области защиты информации.

6.2 Мероприятия по физической защите

Применяемые технические меры защиты информации должны обеспечивать защиту от несанкционированного доступа к информации.

Должна быть организована охрана помещений, в которых размещены элементы ИСПДн и производится обработка персональных данных. Организация режима обеспечения безопасности этих помещений должна обеспечивать сохранность носителей информации и средств защиты информации, и исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Помещения с элементами ИСПДн должны быть оснащены крепкими дверьми с замками и приспособлениями для опечатывания, или соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

6.3 Методы и способы защиты информации от несанкционированного доступа

Для защиты от несанкционированного доступа к информации, рекомендуется применение следующих методов и способов:

- организация физической защиты помещений и технических средств ИСПДн;
- размещение технических средств, предназначенных для обработки персональных данных, в пределах контролируемой зоны;
- ограничение доступа пользователей в помещения, где размещены технические средства ИСПДн, а также хранятся носители информации;
- установление правил доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- управление доступом к защищаемым данным;
- регистрация и учет действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- использование защищенных каналов связи;
- использование средств межсетевого экранирования;
- применение средств антивирусной защиты информации;
- применение средств криптографической защиты информации;
- применение средств анализа защищенности;
- применение средств обнаружения вторжений.

Безопасность персональных данных в ИСПДн должна быть реализована средствами защиты

информации, прошедшими в установленном порядке процедуру оценки соответствия.

ЗАКЛЮЧЕНИЕ

В ходе моделирования угроз безопасности персональных данных были определены перечни объектов среды информатизации и связанные с ними уязвимости. На основании перечня источников угроз и уязвимых звеньев был построен общий перечень угроз безопасности персональных данных.

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» проведена оценка актуальности угроз безопасности персональных данных и определён перечень актуальных угроз для ИСПДн.

Исходя из сформированного перечня актуальных угроз безопасности персональных данных, а также в зависимости от установленного уровня защищённости ПДн, разработаны рекомендации по проведению мероприятий, направленные на обеспечение безопасности персональных данных при их обработке в ИСПДн.

На основании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведения атак, а также с учетом 3-го типа актуальных угроз, уровень криптографической защиты информации, обеспечиваемый криптосредствами ИСПДн, должен соответствовать уровню не ниже КС1 (в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности), при условии соблюдения организационно-режимных и кадрово-режимных мер, действующих в отношении пользователей и на местах эксплуатации криптосредств.

Для обеспечения требований законодательства Российской Федерации, методических и руководящих документов органов государственной власти для ИСПДн должны быть реализованы меры по противодействию актуальным угрозам безопасности информации. Используемые при этом средства защиты информации должны обладать действующими сертификатами соответствия устанавливаемым к данным средствам защиты информации требованиям ФСТЭК России либо ФСБ России.