УТВЕРЖДАЮ
Директор МБОУ лицея
«Технический»
_____ И.А. Бочков

«10» ноября 2014 г.

Частная модель угроз
безопасности персональных данных
в информационной системе персональных данных
«Бухгалтерский и кадровый учёт»

СОГЛАСОВАНО	РАЗРАБОТАЛ
Заместитель директора по информационным технологиям	Инженер по информационной безопасности
_____С.М. Шепелёв	Лучков А.А.

Самара 2014 г.

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

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

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

Информативный сигнал – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

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

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным обра-

зом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и / или выходящей из информационной системы.

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.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каж-

дого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

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

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

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

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

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и / или

осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записи ключей и атрибутов доступа (паролей) на бумажные носители и хранения их вблизи объектов доступа.

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

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспе-

чение информационной системы персональных данных и / или блокировать аппаратные средства.

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

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

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

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

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и

обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

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

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

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

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

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	-	антивирусные средства
АИС	-	автоматизированная информационная система
АРМ	-	автоматизированное рабочее место
ИНН	-	индивидуальный номер налогоплательщика
ИСПДн	-	информационная система персональных данных
ЛВС	-	локальная вычислительная сеть
ЛИС	-	локальная информационная система
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ОУ	-	образовательное учреждение
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПФ	-	пенсионный фонд
ПЭМИН	-	побочные электромагнитные излучения и наводки
РИС	-	распределенная информационная система
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

1 ОБЩИЕ ПОЛОЖЕНИЯ.

Настоящая Частная модель угроз безопасности персональных данных (далее – Модель угроз) в информационной системе персональных данных **«Бухгалтерский и кадровый учёт»** (далее ИСПДн) в Муниципальном бюджетном общеобразовательном учреждении лицее «Технический» городского округа Самара (далее ОУ) разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Совместный приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» (утративший силу в соответствии с Приказом ФСТЭК России N 151, ФСБ России N 786, Минкомсвязи России N 461 от 31.12.2013 "О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных);
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18 февраля 2013 г. № 21.
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г.

В соответствии с п. 2 требований к защите персональных данных при их обработке в информационных системах персональных данных безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Модель угроз формируется и утверждается оператором (ОУ).

Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Разработка модели угроз базируется на следующих принципах:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн).

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗПДн не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификации потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

– Описание угроз.
– Оценку вероятности возникновения угроз.
– Оценку реализуемости угроз.

– Оценку опасности угроз.

– Определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

2 ОПИСАНИЕ ИСПДН «БУХГАЛТЕРСКИЙ И КАДРОВЫЙ УЧЕТ»

2.1 Структура ИСПДн

Таблица 1. Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Информационная система, обрабатывающая ПДн сотрудников ОУ
Структура информационной системы	Локальная ИСПДн
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется (одноточечное)
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах одного здания, являющегося контролируемой зоной ОУ
Дополнительные информация	К персональным данным предъявляются требования конфиденциальности, целостности и доступности

2.2 Состав и структура персональных данных

В целях исполнения обязанностей и реализации прав сторон трудового договора (работника и работодателя) в ОУ обрабатываются персональные данные работников, предусмотренные формой Т-2 (Личная карточка работника), утвержденной Постановлением Госкомстата России от 05.01.2004 № 1, а также другая информация о работнике, в соответствии с «Перечнем персональных данных, обрабатываемых в ОУ».

В данной системе обрабатываются следующие персональные данные сотрудников ОУ, подлежащие защите:

- фамилия, имя, отчество;

- дата, месяц, год рождения;
- пол;
- место рождения;
- серия и номер документа, удостоверяющего личность, дата выдачи и выдавший орган;
- адрес регистрации и адрес проживания;
- семейное положение;
- сведения о состоянии на воинском учёте;
- сведения о финансовом положении;
- сведения об образовании;
- сведения о профессиональных навыках (аттестация, повышение квалификации, профессиональная переподготовка);
- прочие сведения кадрового характера (трудовой стаж, места работы, сведения об отпусках, сведения о льготах);
- ИНН;
- номер телефона, мобильного телефона;
- адрес электронной почты;
- сведения о судимости;
- сведения о состоянии здоровья;
- номер страхового свидетельства;
- государственного пенсионного страхования;
- номер банковской карты.

2.3 Условия расположения основных составляющих АС, обрабатывающих персональные данные.

2.3.1 Территориальное размещение основных составляющих АС.

ИСПДн является локальной, развернутой в пределах одного здания, и состоит из следующих структурных единиц, находящихся в разных кабинетах:

- бухгалтерия;
- отдел кадров;

Обработка информационных потоков ИСПДн осуществляется в 2-х кабинетах, расположенных на 2 этаже здания по адресу: г. Самара, ул. Воронежская, д. 232.

2.3.2 Границы контролируемых зон.

Контролируемой зоной является здание ОУ и прилегающая к нему территория, обнесённая железным забором.

2.4 Топология ИСПДн и конфигурация ее отдельных компонентов.

2.4.1 Топология ИСПДн.

Основными составляющими ИСПДн являются:

- центральный узел обработки данных;
- межсетевой экран - шлюз;
- автоматизированные рабочие места (АРМ) сотрудников.

2.5 Конфигурация отдельных компонентов ИСПДн.

2.5.1 Центральный узел обработки данных.

Центральный узел обработки данных представляет собой ПК, с установленной операционной системой Windows 7 (SP1) в редакции «Корпоративная». Центральный узел является хранилищем файловой информационной базы 1С Предприятие 8.2 конфигурация «Зарплата и кадры бюджетного

учреждения», содержащей персональные данные сотрудников. Всего в ИСПДн используется один центральный узел обработки данных, который расположен в кабинете бухгалтерии и является АРМ главного бухгалтера ОУ.

2.5.2 Межсетевой экран – шлюз.

Межсетевой экран – шлюз представляет собой ПК с установленным программным комплексом Интернет Контроль Сервер. Межсетевой экран – шлюз расположен в служебном помещении (серверной).

2.5.3 АРМ сотрудников.

Основным оборудованием, участвующим в обработке персональных данных, являются АРМ сотрудников. С помощью этого оборудования осуществляется ввод персональных данных в ИСПДн. АРМ сотрудников представляют собой ПК с установленными операционными системами Windows XP (SP3) в редакции «Профессиональная» и Windows 7 (SP1) в редакции «Профессиональная». Работа с ПДн, содержащимися в базе Центрального узла обработки данных, осуществляется средствами платформы 1С Предприятие 8.2.

АРМ сотрудников установлены в кабинетах бухгалтерии и отдела кадров.

2.6 Связи между основными компонентами ИСПДн.

2.6.1 Физические связи.

Структура информационного взаимодействия в ИСПДн реализована на основе собственной локальной Сети передачи данных (далее – СПД), имеющей одноточечное подключение к сетям связи общего пользования и сетям международного информационного обмена, и имеет следующие физические связи:

- АРМ сотрудников подключены к внутренней локальной сети;

- выход в сеть общего пользования является одноточечным и осуществляется посредством модемного подключения, защищен межсетевым экраном – шлюзом. Данный канал связи предназначен для отправки консолидированных отчетов в государственные органы ФНС, ФСС, ПФР, Росстат.

2.6.2 Технологические связи.

В процессе обработки персональных данных в ИСПДн используются следующие технологии:

- персональные данные хранятся на центральном узле обработки данных в специально предназначенной для этого СУБД;
- ПО, обеспечивающее передачу персональных данных от конечного периферийного оборудования до СУБД, работает по протоколу TCP/IP;

2.6.3 Функциональные связи.

Введенные на АРМ сотрудников данные пересылаются непосредственно на центральный узел обработки данных встроенными средствами ПО 1С Предприятие.

В ИСПДн используется одна база ПДн, принадлежащая ОУ, данные, содержащиеся в этой базе, не являются обезличенными, часть этих данных может быть предоставлена третьим лицам.

Структура ИСПДн приведена на схеме (см. Рисунок 1).

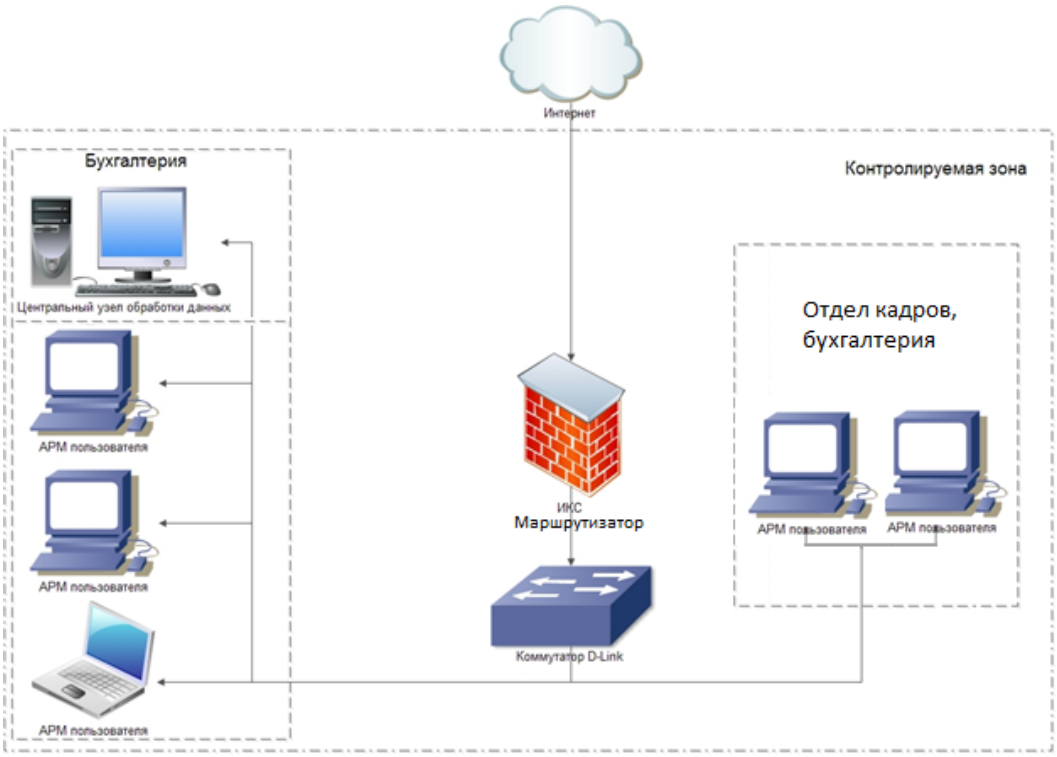

Рисунок 1. Схема ИСПДн.

2.7 Технические средства, участвующие в обработке персональных данных в ИСПДн.

В обработке персональных данных участвуют следующие технические средства:

- АРМ сотрудников;
- Межсетевой экран – шлюз «Интернет Контроль Сервер»;

Кроме того, в обработке персональных данных участвует следующее сетевое оборудование: коммутатор D-Link.

2.8 Общесистемные и прикладные программные средства, участвующие в обработке персональных данных.

В обработке персональных данных участвует следующее общесистемное программное обеспечение:

- ОС Windows XP (SP3) в редакции «Профессиональная»;
- ОС Windows 7 (SP1) в редакциях «Профессиональная», «Корпоративная».

В обработке персональных данных участвует следующее прикладное программное обеспечение:

- 1С Предприятие 8.2, конфигурация «Зарплата и кадры бюджетного учреждения»;
- Microsoft Office Professional Plus 2010.

Антивирусную защиту обеспечивает ПО Антивирус Касперского.

2.9 Режим и степень участия персонала в обработке персональных данных.

Обработка персональных данных на всех АРМ, являющихся компонентами ИСПДн, осуществляется в однопользовательском режиме.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице 2.

Таблица 2. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	сбор систематизация накопление хранение уточнение использование уничтожение
Администратор безопасности	Обладает правами Администратора ИСПДн.	сбор систематизация

	Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	накопление хранение уточнение использование уничтожение
Операторы ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. Не имеет полномочий вносить модификации в настройки какого-либо оборудования, системного и прикладного ПО.	сбор систематизация накопление хранение уточнение использование уничтожение

Доступ к ИСПДн имеют только сотрудники ОУ, определённые Перечнем сотрудников, допущенных к обработке персональных данных в информационной системе персональных данных «Бухгалтерский и кадровый учёт».

Предоставление доступа к ИСПДн сотруднику ОУ осуществляется на основании приказа о приёме на работу на определённые должности или распоряжение руководителя о предоставлении доступа сотруднику к ИСПДн

Причиной для прекращения доступа сотрудников ОУ к ИСПДн является увольнение сотрудника, либо распоряжение руководителя о прекращении доступа сотрудника к ИСПДн.

2.10 Тип ИСПДн

Угрозы безопасности персональных данных (УБПДн) зависят от типа ИСПДн.

По структуре ИСПДн является комплексом автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы).

По наличию подключений к сетям связи ИСПДн является информационной системой, которая имеет подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

По режиму обработки персональных данных ИСПДн является многопользовательской.

По разграничению прав доступа пользователей ИСПДн является системой с разграничением прав доступа.

В зависимости от местонахождения технических средств ИСПДн является системой, все технические средства которой находятся в пределах Российской Федерации.

Исходя из вышеперечисленных характеристик ИСПДн, можно определить, что ИСПДн является ЛИС II типа – локальная информационная система, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

2.11 Исходный уровень защищенности ИСПДн

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

Исходная степень защищенности определяется следующим образом.

1) **(Y1=0)**. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения но первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2) **(Y1=5)**. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положи-

тельные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3) **(Y1=10)**. ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

Таблица 3. Характеристики ИСПДн, определяющие исходный уровень защищенности.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. ***По территориальному размещению:***			
локальная ИСПДн, развернутая в пределах одного здания.	+	-	-
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая одноточечный выход в сеть общего пользования.	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача.	-	-	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн.	–	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн.	+	-	-
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).	-	-	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая часть ПДн.	-	+	-

В соответствии с таблицей 3, не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", следовательно Y_1=5.

3 ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УБПДН

3.1 Классификация угроз безопасности

Перечень угроз, уязвимостей и технических каналов утечки информации сформирован в соответствии с требованиями руководящих документов ФСТЭК России.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн обрабатываемым в ИСПДн.

ИСПДн ОУ представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными элементами ИСПДн являются:

- персональные данные, обрабатываемые в ИСПДн;
- информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
- технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации (СЗИ), включая СКЗИ;
- вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
- документация на СКЗИ и на технические и программные компоненты ИСПДн;
- ключевая, аутентифицирующая и парольная информация;

- помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;
- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;
- носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;
- носитель вредоносной программы.

3.2 Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

– внешние нарушители – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

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

3.2.1 Внешний нарушитель

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

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как:

− канал утечки акустической информации отсутствует, потому что в ИСПДн отсутствуют функции голосового ввода ПДн в информационную систему и функции воспроизведения ПДн акустическими средствами информационной системы;

− канал утечки видовой информации перекрывается организационными и инженерно-техническими мерами (т.е. ИСПДн расположена в пределах КЗ ОУ, доступ в здание ОУ ограничен, помещения, в которых находятся ПДн, находятся на 2-м этаже здания, доступ туда ограничен, окна данных помещений оборудованы жалюзи);

− утечка информации за счёт ПЭМИН является маловерояной, т.к. ИСПДн расположена в пределах КЗ ОУ, доступ в здание ОУ ограничен, объем и ценность информации, хранимой и обрабатываемой в ИСПДн, являются недостаточными для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на получение информации по техниче-

ским каналам утечки, в связи с очень высокой стоимостью средств съема информации в результате регистрации ПЭМИН.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию, обрабатываемую в ИСПДн, представленную в виде бит, байт, IP-протоколов, файлов и других логических структур.

3.2.2 Внутренний нарушитель

К такому виду нарушителя могут относиться:

– пользователи ИСПДн, т.е. сотрудники, имеющие право доступа к ИСПДн (категория I);

– сотрудники, не имеющие права доступа к ИСПДн (категория II);

– администраторы ИСПДн (категория III);

– разработчики и поставщики программно-технических средств, расходных материалов, услуг (категория IV).

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

Лица категорий I и III хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам данных категорий ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

3.2.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

– *общая информация* – информации о назначении и общих характеристиках ИСПДн;

– *эксплуатационная информация* – информация, полученная из эксплуатационной документации;

В частности, нарушитель может иметь:

– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

– сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

– данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

– данные о реализованных в ПСЗИ принципах и алгоритмах;

– исходные тексты программного обеспечения ИСПДн;

– сведения о возможных каналах реализации угроз;

– информацию о способах реализации угроз.

Предполагается, что лица категории I владеют только эксплуатационной информацией, что обеспечивается организационными мерами.

Предполагается, что лица категории III обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн.

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

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

3.2.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

– аппаратные компоненты СЗПДн;

– доступные в свободной продаже технические средства и программное обеспечение;

– специально разработанные технические средства и программное обеспечение.

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

Вместе с тем предполагается, что нарушитель не имеет:

– средств перехвата в технических каналах утечки;

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

– средств воздействия на источники и через цепи питания;

– средств воздействия через цепи заземления;

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

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории IV.

Необходимо определить всех потенциальных нарушителей, не имеющих доступа в ИСПДн, всех пользователей ИСПДн и определить их категорию.

3.3 Классификация уязвимостей ИСПДн

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

3.4 Определение вероятности реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

– **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

– **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

– **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы.

3.5 Угрозы утечки информации по техническим каналам

3.5.1 Угрозы утечки акустической (речевой) информации

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

В ИСПДн ОУ функции голосового ввода ПДн и функции воспроизведения ПДн акустическими средствами отсутствуют. Поэтому для всех видов нарушителей реализация угрозы является маловероятной.

3.5.2 Угрозы утечки видовой информации

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

В ОУ введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи, поэтому реализация угрозы является маловероятной.

3.5.3 Угрозы утечки информации по каналам ПЭМИН

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

Угрозы данного класса маловероятны, т.к. размер контролируемой зоны большой и элементы ИСПДн находятся в самом центре здания и экранируются несколькими несущими стенами, а паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

3.6 Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа

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

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

3.6.1 Кража и уничтожение носителей информации

Угроза может осуществляться всеми видами нарушителей.

В ОУ введен контроль доступа в контролируемую зону, установлена охранная сигнализация и система видеонаблюдения, двери закрываются на замок, установлены решетки на первых этажах здания, ведется учет и хранение носителей в сейфе, поэтому для ИСПДн вероятность реализации угрозы – является маловероятной.

3.6.2 Кража физических носителей ключей и атрибутов доступа

Угроза может осуществляться всеми видами нарушителей.

В ОУ введен контроль доступа в контролируемую зону, установлена охранная сигнализация и система видеонаблюдения, двери закрываются на замок, установлены решетки на первых этажах здания, ведется учет и хране-

ние носителей в сейфе, введена парольная политика, поэтому для ИСПДн вероятность реализации угрозы – является низкой.

3.6.3 Утрата носителей информации

Угроза осуществляется внутренними нарушителями, являющимися пользователями ИСПДн, вследствие человеческого фактора.

В ОУ осуществляется учет носителей информации и пользователи проинструктированы о действиях в случаях утраты носителей, то для всех видов ИСПДн вероятность реализации угрозы – является маловероятной.

3.6.4 Утрата и компрометация ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают простые 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.

В ОУ введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за выполнением правил политик, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, то для всех видов ИСПДн вероятность реализации угрозы – является низкой.

3.7 Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств

3.7.1 Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа

Угроза осуществляется внешними нарушителями и внутренними нарушителями категорий II и IV там, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В ОУ введен контроль доступа в контролируемую зону, установлена охранная сигнализация и система видеонаблюдения, двери закрываются на замок, установлены решетки на первых и последних этажах здания, поэтому для ИСПДн вероятность реализации угрозы – является маловероятной.

3.7.2 Утечка информации через порты ввода/вывода

Угроза осуществляется внутренними нарушителями категорий I и IV.

Угроза реализуется путем подключения съемных носителей к компьютеру и несанкционированного копирования на них информации.

В ОУ доступ к носителям ПДн ограничен, пользователи ознакомлены с политикой безопасности, для ИСПДн вероятность реализации угрозы – является низкой.

3.7.3 Воздействие 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 ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– 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.

В ОУ на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, поэтому для ИСПДн вероятность реализации угрозы – является низкой.

3.7.4 Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями категорий I и IV.

В ОУ введено разграничение прав пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО, вероятность реализации угрозы – является низкой.

При отсутствии разграничения прав на установку ПО, вероятность реализации угрозы должна быть пересмотрена, и необходимо принять меры по организации разграничения прав пользователей.

3.7.5 Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных

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

В ОУ осуществляется контроль действий пользователей и разработчиков, системное и прикладное ПО установленное в элементах ИСПДн сертифицировано ФСТЭК, имеется одноточечное подключение к сетям общего доступа и (или) международного обмена, защищаемое межсетевым экраном, вероятность реализации угрозы – является низкой.

3.7.6 Создание учетных записей теневых пользователей и неучтенных точек доступа в систему

Угроза осуществляется внутренними нарушителями категорий I и IV.

Угроза реализуется путем несанкционированного создания неучтенных точек доступа в систему (например, несанкционированное подключение нового компьютера к локальной сети), а также создание нерабочих учетных записей (тестовых, временных и т.д.).

Вероятность реализации угрозы – является маловероятной.

3.8 Угрозы несанкционированного доступа к информации по каналам связи

3.8.1 Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны

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. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

3.8.2 Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, 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.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

3.8.3 Угроза выявления паролей по сети

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для

себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность реализации угрозы – является низкой.

3.8.4 Угрозы типа «Отказ в обслуживании»

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

Могут быть выделены несколько разновидностей таких угроз:

– скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

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

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

В ОУ обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, за исключением отправки периодической бухгалтерской отчетности в контролирующие органы, частично содержащей ПДн, поэтому вероятность реализации угрозы – является маловероятной.

3.8.5 Угрозы внедрения по сети вредоносных программ

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

удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

– программы подбора и вскрытия паролей;
– программы, реализующие угрозы;
– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
– программы-генераторы компьютерных вирусов;
– программы, демонстрирующие уязвимости средств защиты информации и др.

В ОУ на всех АРМ ИСПДн установлена антивирусная защита, доступ в сети общего пользования и международного обмена защищен межсетевым экраном, вероятность реализации угрозы – является маловероятной.

3.8.6 Утечка информации, передаваемой с использованием протоколов беспроводного доступа

Угроза реализуется путем перехвата информации, передаваемой по беспроводным сетям.

В ОУ отсутствуют элементы ИСПДн, передающие информацию с использованием протоколов беспроводного доступа,поэтому вероятность реализации угрозы – является маловероятной.

3.8.7 Перехват, модификация закрытого ключа ЭЦП

Угроза реализуется путем получения доступа к закрытому ключу ЭЦП либо путем перехвата закрытого ключа ЭЦП.

Вероятность реализации угрозы – является маловероятной.

3.8.8 Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации

такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

В ОУ на всех АРМ ИСПДн установлена антивирусная защита, до-ступ в сети общего пользования и международного обмена защищен межсетевым экраном, вероятность реализации угрозы – является маловероятной.

3.9 Угрозы антропогенного характера

3.9.1 Разглашение информации

Угроза осуществляется внутренними нарушителями категорий I и III.

Угроза реализуется путем несанкционированной передачи информации третьим лицам.

В ОУ пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении, поэтому вероятность реализации угрозы – является низкой.

3.9.2 Сокрытие ошибок и неправомерных действий пользователей и администраторов

Угроза реализуется внутренними нарушителями категорий I и III.

В ОУ осуществляется контроль действий пользователей, вероятность реализации угрозы – является маловероятной.

3.9.3 Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей

Угроза реализуется внутренними нарушителями категории III.

Угроза реализуется вследствие халатного отношения ответственного лица к своим должностным обязанностям.

В ОУ осуществляется контроль действий ответственных лиц, вероятность реализации угрозы – является маловероятной.

3.9.4 Угроза нарушения политики предоставления и прекращения доступа

Угроза реализуется внутренними нарушителями категории III.

Угроза реализуется при отсутствии процедуры удаления устаревших, неучтенных или недействующих учетных записей пользователей или несанкционированного предоставления прав доступа.

Вероятность реализации угрозы повышается при отсутствии контроля действий администраторов.

Вероятность реализации угрозы – является маловероятной.

3.9.5 Непреднамеренная модификация (уничтожение) информации

Угроза реализуется внутренними нарушителями категорий I и III.

Угроза реализуется путем непреднамеренного воздействия на элементы ИСПДн или содержащуюся в ней информацию.

В ОУ осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн, вероятность реализации угрозы – является маловероятной.

3.9.6 Непреднамеренное отключение средств защиты

Угроза реализуется внутренними нарушителями категорий I и III.

Угроза реализуется путем случайного отключения средств защиты (антивирусного ПО, межсетевых экранов и т.д.).

Вероятность реализации угрозы повышается при отсутствии контроля доступа в контролируемую зону и к настройкам режимов средств защиты, а так же неосведомленности пользователей о работе с ИСПДн.

Вероятность реализации угрозы для всех видов ИСПДн – является маловероятной.

3.10 Угрозы воздействия непреодолимых сил

3.10.1 Стихийное бедствие

Угроза осуществляется вследствие возникновения различного рода природных катаклизмов (землетрясение, затопление и прочее).

В ОУ установлена пожарная сигнализация и система речевого оповещения, сотрудники проинструктированы о действиях в случае возникновения внештатных ситуаций, вероятность реализации угрозы – является маловероятной.

3.10.2 Выход из строя аппаратно-программных средств

Угроза реализуется вследствие окончания срока эксплуатации аппаратно-программных средств, нерегулярных проверок данных средств и перебоев в электропитании.

В ОУ производится своевременная замена устаревших аппаратно-программных средств, регулярные проверки аппаратно-программных средств и установлены элементы бесперебойного питания, вероятность реализации угрозы – является маловероятной.

3.10.3 Аварии (пожар, потоп, случайное отключение электричества)

Угроза осуществляется вследствие возникновения различного рода аварий в пределах контролируемой зоны.

В ОУ производится своевременная замена устаревшего оборудования, коммуникаций и т.д., проводятся их регулярные проверки, установлены элементы бесперебойного питания, вероятность реализации угрозы – является маловероятной.

3.11 Реализуемость угроз

По итогам оценки уровня защищенности (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 УБПДн представлена в таблице.

Таблица 3. Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа		
2.1. Кража и уничтожение носителей информации	0,25	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	0,35	средняя
2.3. Утрата носителей информации	0,25	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	0,35	средняя
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств		
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	0,25	низкая
3.2. Утечка информации через порты ввода/вывода	0,35	средняя
3.3. Воздействие вредоносных программ (вирусов)	0,35	средняя

3.4. Установка ПО, не связанного с исполнением служебных обязанностей	0,35	средняя
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	0,25	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	0,25	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи		
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	0,25	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	низкая
4.3. Угрозы выявления паролей по сети	0,35	средняя
4.4. Угрозы типа «Отказ в обслуживании»	0,25	низкая
4.5. Угрозы внедрения по сети вредоносных программ	0,25	низкая
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	0,25	низкая
4.7. Перехват, модификация закрытого ключа ЭЦП	0,25	низкая
4.8. Угрозы удаленного запуска приложений	0,25	низкая
5. Угрозы антропогенного характера		
5.1. Разглашение информации	0,35	средняя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	0,25	низкая

5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	0,25	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	0,25	низкая
5.5. Непреднамеренная модификация (уничтожение) информации	0,25	низкая
5.6. Непреднамеренное отключение средств защиты	0,25	низкая
6. Угрозы воздействия непреодолимых сил		
6.1. Стихийное бедствие	0,25	низкая
6.2. Выход из строя аппаратно-программных средств	0,25	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	0,25	низкая

3.12 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который 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.

Оценка опасности УБПДн представлена таблице.

Таблица 4. Опасность УБПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая

1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	низкая
2.2. Кража физических носителей ключей и атрибутов доступа	средняя
2.3. Утрата носителей информации	низкая
2.4. Утрата и компрометация ключей и атрибутов доступа	средняя
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	низкая
3.2. Утечка информации через порты ввода/вывода	средняя
3.3. Воздействие вредоносных программ (вирусов)	средняя
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	низкая
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	низкая
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	низкая
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	низкая
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
4.3. Угрозы выявления паролей по сети	средняя
4.4. Угрозы типа «Отказ в обслуживании»	низкая
4.5. Угрозы внедрения по сети вредоносных программ	средняя
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	низкая
4.7. Перехват, модификация закрытого ключа ЭЦП	низкая

4.8. Угрозы удаленного запуска приложений	низкая
5. Угрозы антропогенного характера	
5.1. Разглашение информации	средняя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	низкая
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	низкая
5.4. Угроза нарушения политики предоставления и прекращения доступа	низкая
5.5. Непреднамеренная модификация (уничтожение) информации	низкая
5.6. Непреднамеренное отключение средств защиты	низкая
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	низкая
6.2. Выход из строя аппаратно-программных средств	низкая
6.3. Аварии (пожар, потоп, случайное отключение электричества)	низкая

3.13 Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 5. Правила определения актуальности УБПДн

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

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 6. Актуальность УБПДн

Тип угроз безопасности ПДн	Актуальность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа	
2.1. Кража и уничтожение носителей информации	неактуальная
2.2. Кража физических носителей ключей и атрибутов доступа	актуальная
2.3. Утрата носителей информации	неактуальная
2.4. Утрата и компрометация ключей и атрибутов доступа	актуальная
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств	
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	неактуальная
3.2. Утечка информации через порты ввода/вывода	актуальная
3.3. Воздействие вредоносных программ (вирусов)	актуальная
3.4. Установка ПО, не связанного с исполнением служебных обязанностей	неактуальная
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	неактуальная
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	неактуальная
4. Угрозы несанкционированного доступа к информации по каналам связи	
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны	неактуальная
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений	неактуальная

и др.	
4.3. Угрозы выявления паролей по сети	актуальная
4.4. Угрозы типа «Отказ в обслуживании»	неактуальная
4.5. Угрозы внедрения по сети вредоносных программ	неактуальная
4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа	неактуальная
4.7. Перехват, модификация закрытого ключа ЭЦП	неактуальная
4.8. Угрозы удаленного запуска приложений	неактуальная
5. Угрозы антропогенного характера	
5.1. Разглашение информации	актуальная
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	неактуальная
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	неактуальная
5.4. Угроза нарушения политики предоставления и прекращения доступа	неактуальная
5.5. Непреднамеренная модификация (уничтожение) информации	неактуальная
5.6. Непреднамеренное отключение средств защиты	неактуальная
6. Угрозы воздействия непреодолимых сил	
6.1. Стихийное бедствие	неактуальная
6.2. Выход из строя аппаратно-программных средств	неактуальная
6.3. Аварии (пожар, потоп, случайное отключение электричества)	неактуальная

Были выявлены следующие актуальные угрозы:

- кража физических носителей ключей и атрибутов доступа;
- утрата и компрометация ключей и атрибутов доступа;
- утечка информации через порты ввода/вывода;
- воздействие вредоносных программ (вирусов);
- угрозы выявления паролей по сети;
- разглашение информации.

Для снижения опасности реализации актуальных УБПДн должны быть осуществлены следующие мероприятия:

– установка антивирусной защиты;

– использование межсетевого экрана;

– парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

– назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;

– инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;

– учет носителей информации, используемых в ИСПДн;

– учет ключевых элементов, используемых в ИСПДн;

– осуществление резервирования ключевых элементов ИСПДн;

– осуществление резервирования носителей информации ИСПДн;

– организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

3.14 Модель угроз безопасности

Исходный класс защищенности – средний

Таблица 7. Угрозы безопасности

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим Инструкция пользователя
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная	Генераторы пространственного зашумления Генератор шума по цепи электро-	Контур заземления

					питания	
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа						
2.1. Кража и уничтожение носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Хранение в сейфе	Учет носителей информации
					Шифрование данных	
2.2. Кража физических носителей ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная	Охранная сигнализация	Инструкция пользователя
					Хранение в сейфе	Учет носителей ключей и атрибутов доступа
2.3. Утрата носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Резервирование носителей информации	Инструкция пользователя
					Шифрование данных	Инструкция администратора безопасности
2.4. Утрата и компрометация ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя
						Инструкция администратора

						безопасности
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств						
3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты
						Разрешительная система допуска
3.2. Утечка информации через порты ввода/вывода	Низкая	Средняя	Средняя	Актуальная	Изолирование портов ввода/вывода	Инструкция пользователя
3.3. Воздействие вредоносных программ (вирусов)	Низкая	Средняя	Средняя	Актуальная	Антивирусное ПО	Инструкция пользователя
						Инструкция ответственного
						Инструкция администратора безопасности
						Инструкция по антивирусной защите
						Акт установки средств защиты

3.4. Установка ПО не связанного с исполнением служебных обязанностей	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция ответственного
3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Низкая	Неактуальная		Сертификация
3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему	Маловероятно	Низкая	Низкая	Неактуальная	Система управления доступом	Инструкция пользователя Инструкция ответственного Инструкция администратора безопасности
4. Угрозы несанкционированного доступа к информации по каналам связи						
4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зо-	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Инструкция пользователя Инструкция администратора безопасности

ны						Акт установки средств защиты
4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
4.3. Угрозы выявления паролей по сети	Низкая	Средняя	Средняя	Актуальная	Межсетевой экран	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
4.4. Угрозы типа «Отказ в обслуживании»	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Инструкция пользователя Инструкция администратора

						безопасности
						Резервирование
4.5. Угрозы внедрения по сети вредоносных программ	Маловероятно	Низкая	Низкая	Неактуальная	Антивирусное ПО Межсетевой экран	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
4.6. Утечка информации, передаваемой с использованием протоколов беспроводного доступа	Маловероятно	Низкая	Низкая	Неактуальная	Шифрование информации	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты
4.7. Перехват, модификация закрытого ключа ЭЦП	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Инструкция пользователя
						Инструкция администратора безопасности
						Акт установки средств защиты

4.8. Угрозы удаленного запуска приложений	Маловероятно	Низкая	Низкая	Неактуальная	Межсетевой экран Антивирусное ПО	Инструкция пользователя Инструкция администратора безопасности Акт установки средств защиты
5. Угрозы антропогенного характера						
5.1. Разглашение информации	Низкая	Средняя	Средняя	Актуальная		Договор о неразглашении Инструкция пользователя
5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов	Маловероятно	Низкая	Низкая	Неактуальная		Договор о неразглашении Инструкция пользователя
5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная		Договор о неразглашении Инструкция пользователя

5.4. Угроза нарушения политики предоставления и прекращения доступа	Маловероятно	Низкая	Низкая	Неактуальная		Договор о неразглашении Инструкция пользователя
5.5. Непреднамеренная модификация (уничтожение) информации	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты Резервное копирование	Инструкция пользователя
5.6. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
6. Угрозы воздействия непреодолимых сил						
6.1. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация Система голосового оповещения	Инструкции по безопасности
6.2. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная	Устройство бесперебойного питания	Резервирование Инструкции по безопасности

6.3. Аварии (пожар, потоп, случайное отключение электричества)	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация Система голосового оповещения	Инструкции по безопасности

4 ЗАКЛЮЧЕНИЕ

В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" ИСПДн **«Бухгалтерский и кадровый учет»** является информационной системой, обрабатывающей специальные категории персональных данных, т.к. в ней обрабатываются данные, касающиеся состояния здоровья.

ИСПДн **«Бухгалтерский и кадровый учет»** является информационной системой, обрабатывающей персональные данные сотрудников оператора.

Для ИСПДн **«Бухгалтерский и кадровый учет»** актуальны угрозы 3-го типа, т.к. для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Для ИСПДн **«Бухгалтерский и кадровый учет»** актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных менее чем 100000 субъектов персональных данных, являющихся сотрудниками оператора, поэтому необходимо обеспечить 3-й уровень защищенности персональных данных при их обработке в информационной системе.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) 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;

б) обеспечение сохранности носителей персональных данных;

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

г) 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;

д) назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Уровень защищенности персональных данных при их обработке в ИСПДн **«Бухгалтерский и кадровый учет»** может быть пересмотрен:

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

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации для обеспечения 3 уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;
- межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.

Состав и содержание мер по, обеспечению безопасности персональных данных, необходимых для обеспечения 3-го уровня защищенности персональных данных, утверждённые приказом ФСТЭК России от 18 февраля 2013 г. № 21, описаны в Приложении 1.

ПРИЛОЖЕНИЕ 1

Состав и содержание мер по, обеспечению безопасности персональных данных, необходимых для обеспечения 3-го уровня защищенности персональных данных

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Реализация в ИСПДн
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Средства ОС и средства прикладного ПО
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Парольная политика, обязанности администратора безопасности
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	Парольная политика, обязанности администратора безопасности
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Средства ОС
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В ИСПДн отсутствуют внешние пользователи
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	Инструкция администратора ИСПДн
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Положение о разграничении доступа к ПДн
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	Межсетевой экран ИКС

УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Положение о разграничении доступа к ПДн, Перечень сотрудников допущенных к обработке ПДн
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Положение о разграничении доступа к ПДн, Перечень сотрудников допущенных к обработке ПДн
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Парольная политика, средства ОС
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Средства ОС
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Средства ОС
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Внешний доступ запрещён
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Технологии беспроводного доступа не используются
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Мобильные технические средства не используются
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Взаимодействие с информационными системами сторонних организаций запрещено, за исключением контролирующих органов
IV. Защита машинных носителей персональных данных (ЗНИ)		
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) или обезличивания	Средства ОС
V. Регистрация событий безопасности (РСБ)		

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Инструкция администратора по безопасности
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Инструкция администратора по безопасности
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Инструкция администратора по безопасности
РСБ. 7	Защита информации о событиях безопасности	Инструкция администратора по безопасности
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Антивирус
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Средства антивирусного ПО
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Инструкция администратора ИСПДН, средства ОС
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Инструкция администратора ИСПДН, средства ОС
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Инструкция администратора ИСПДН, средства ОС
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Инструкция администратора ИСПДН, средства ОС
XI. Защита среды виртуализации (ЗСВ)		
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Средства виртуализации не применяются
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Средства виртуализации не применяются
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Средства виртуализации не применяются
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Средства виртуализации не применяются

ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Средства виртуализации не применяются
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	Ограничение доступа в контролируемую зону, двери запираются на замки, охранная сигнализация
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Устройства отображения информации размещены соответствующим образом
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	Межсетевой экран
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Беспроводные соединения не используются
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Положение о разграничении доступа
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Резервирование, инструкция администратора ИСПДн

УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	Инструкция администратора ИСПДн
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Журнал учёта изменений в конфигурации ИСПДН