Муниципальная организация дополнительного образования
«Центр дополнительного образования» городского округа Прохладный КБР

УТВЕРЖДЕНА
приказом директора МОДО ЦДО
от «05 » июня 2017 г. № 140-д
_____ С.А. Цаголова

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных информационной системы персональных данных МОДО ЦДО

г. Прохладный
2017 г.

Оглавление

1. Обозначения и сокращения....3
2. Термины и определения....4
3. Нормативные и библиографические ссылки....8
4. Общие положения....8
5. Описание информационной системы персональных данных....10
6. Принципы модели угроз....12
7. Модель нарушителя безопасности персональных данных....13
8. Определение класса средств криптографической защиты информации....18
9. Определение актуальных угроз безопасности персональных данных в информационной системе персональных данных....18
10. Заключение....20

1. Обозначения и сокращения

АРМ	– автоматизированное рабочее место
ИР	– информационный ресурс
ИСПДн	– информационная система персональных данных
КЗ	– контролируемая зона
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевой экран
НДВ	– недокументированные (недекларированные) возможности
НЖМД	– накопитель на жестком магнитном диске
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПК	– программный комплекс
ПО	– программное обеспечение
САВЗ	– средство антивирусной защиты
СВТ	– средство вычислительной техники
СЗИ	– средство защиты информации
СЗИ от НСД	– средство защиты информации от несанкционированного доступа
СЗПДн	– система защиты персональных данных
СКЗИ	– средство криптографической защиты информации
СФ	– среда функционирования СКЗИ
УБПДн	– угрозы безопасности персональных данных

2. Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность информации (данных) – состояние защищённости информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование доступа к информации – прекращение или затруднение доступа законных пользователей к информации.

Вредоносная программа (программное обеспечение) – программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа и или деструктивного воздействия на информацию или ресурсы информационной системы нарушение их целостности и/или доступности.

Доступ к информации – возможность получения информации и её использования.

Доступность информации (ресурсов информационной системы) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами актами или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и или воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

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

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

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

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

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

Источник угрозы безопасности информации – субъект, физическое лицо, материальный объект или физическое явление, являющийся непосредственной причиной возникновения угрозы безопасности информации.

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

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

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Машинный носитель информации – материальный носитель, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами.

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

Модель угроз безопасности – это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Модификация информации – целенаправленное изменение формы представления и содержания информации.

Нарушитель безопасности информации – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Недекларированные возможности (программного обеспечения) – функциональные возможности программного обеспечения, не описанные или не

соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и (или) целостности обрабатываемой информации.

Несанкционированный доступ к информации – доступ к информации ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

Потенциал нарушителя – мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

Предоставление информации – действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц.

Программная закладка – скрытно внесенный в программное обеспечение

функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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

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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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 актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз.

Уязвимость программного обеспечения – ошибка в программном обеспечении, способная напрямую быть использована хакером для получения доступа к системе или сети.

Целостность информации – состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и (или) непреднамеренного воздействия на нее.

3. Нормативные и библиографические ссылки

Настоящий документ составлен в соответствии и на основании следующих документов:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены приказом ФСТЭК России от 18 февраля 2013 г.).

– «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).

– «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России).

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (утверждён приказом ФСБ России 10 июля 2014г. ФСБ России № 378).

– «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/5-144).

– Банк данных угроз безопасности информации www.bdu.fstec.ru.

4. Общие положения

Настоящая «Частная модель угроз безопасности персональных данных информационной системы МОДО ЦДО» (далее – Модель угроз) содержит

систематизированный перечень угроз безопасности ПДн информационной системы персональных данных (далее – ИСПДн).

Модель угроз содержит данные по УБПДн, реализация которых может привести к нарушению безопасности ПДн, обрабатываемых в ИСПДн.

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

Разработка Модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности ПДн, обрабатываемых в ИСПДн, и проектирования СЗПДн.

Модель угроз необходима для:

– анализа защищённости ИСПДн от УБПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

– разработки СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием мер по обеспечению безопасности ПДн, предусмотренных для соответствующего уровня защищённости ПДн;

– проведения мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи ПДн лицам, не имеющим права доступа к ПДн;

– недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

– контроля (мониторинга) за обеспечением уровня защищённости ПДн, обрабатываемых в ИСПДн.

В Модели угроз представлено описание ИСПДн и её структурно-функциональных характеристик, описание УБПДн, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации УБПДн и последствий от нарушения свойств безопасности информации, а также произведён анализ УБПДн.

Анализ УБПДн включает:

– описание угроз;

– оценку вероятности возникновения угроз;

– оценку реализуемости угроз;

– оценку опасности угроз;

– определение актуальности угроз.

В процессе функционирования ИСПДн, предполагается конкретизировать и пересматривать данную Модель угроз.

УБПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых уязвимостей, источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Модель угроз может быть пересмотрена:

– на основе периодически проводимых анализа и оценки УБПДн с учетом особенностей и (или) изменений ИСПДн;

– по результатам мероприятий по контролю за выполнением требований по защите информации в ИСПДн.

5. Описание информационной системы персональных данных

5.1. Назначение и состав информационной системы персональных данных

В ИСПДн обрабатываются ПДн субъектов ПДн МОДО ЦДО, к которым относятся:

– лица, являющиеся сотрудниками МОДО ЦДО;

– лица, обучающиеся в МОДО ЦДО;

– лица, которым выданы документы государственного образца.

ИСПДн обеспечивает неавтоматизированный информационный обмен ПДн с:

– МКУ «Управление бухгалтерского учета г.о. Прохладный КБР»;

– МУ «Управление образования местной администрации г.о. Прохладный КБР».

Целями обработки ПДн в ИСПДн являются:

– приём на работу в МОДО ЦДО;

– предоставление образовательных услуг.

В ИСПДн в отношении ПДн осуществляются следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление), удаление.

Режим обработки ПДн – многопользовательский с разными правами доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

Обработка ПДн осуществляется в смешанном виде (с использованием средств автоматизации и без использования средств автоматизации).

Объектами защиты в ИСПДн являются: машинные носители информации, программное и аппаратное обеспечение, информационные ресурсы.

ИСПДн располагается в кабинете директора МОДО ЦДО.

Основные технические характеристики АРМ, входящего в состав ИСПДн, приведены в таблице 1.

Таблица 1 – Технические характеристики АРМ ИСПДн

Имя компьютера	Процессор	Оперативная память (RAM), доступная ОС, МБ	Общая ёмкость накопителей, ГБ	IP-адрес
direktor	Intel Celeron CPUJ1800, 2410 MHz	2000	500	192.168.2.55

Для обработки ПДн используется ПО, указанное в таблице 2.

Таблица 2 – ПО, используемое для обработки ПДн

Наименование	Назначение
Microsoft Windows 7 Professional Service Pack 1	Операционная система
Kaspersky Endpoint Security	Антивирус
7-Zip 16.02	Архиватор
Adobe Reader XI – Russian	ПО для просмотра файлов в формате PDF
Google Chrome	Браузер
Microsoft Office профессиональный плюс 2007	Пакет офисных приложений

5.2. Порядок ввода, хранения и передачи персональных данных в информационной системе персональных данных

Получение ПДн происходит непосредственно от субъекта ПДн.

В процессе обработки ПДн хранятся на бумажном носителе, жёстком диске АРМ.

Для передачи ПДн применяются флэш-накопители.

Трансграничная передача ПДн не осуществляется.

5.3. Режим и степень участия субъектов в обработке персональных данных

В процессе обработки ПДн участвуют следующие категории субъектов:

– пользователи ИСПДн МОДО ЦДО;

– системный администратор МОДО ЦДО.

Пользователями ИСПДн являются административно-управленческий и педагогический персонал МОДО ЦДО, в должностные обязанности которых входит обработка ПДн.

Системный администратор МОДО ЦДО выполняет обслуживание и настройку, поддерживает работоспособность АРМ, выполняет установку и настройку ПО, обслуживание и конфигурирование, разграничивает права доступа субъектов доступа к объектам доступа в ИСПДн.

5.4. Реализованные меры защиты

Разработано и утверждено Положение об обработке персональных данных работников и обучающихся МОДО ЦДО. Приказом назначено лицо, ответственное за

организацию обработки персональных данных. Опубликован и размещен на сайте организации документ, определяющий Политику в отношении обработки персональных данных, а также лист согласия на обработку персональных данных. Разработаны локальные акты по вопросам обработки персональных данных. Осуществляется внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152- ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных. Разработана частная модель угроз безопасности в информационной системе. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним. Средства обеспечения безопасности: используются только сертифицированные средства защиты информации (Базовый пакет Microsoft (операционная система, набор офисных приложений), антивирус Kaspersky Endpoint Security. Составлен перечень сведений конфиденциального характера в МОДО ЦДО, назначен ответственный за организацию обработки ПДн. Персональные данные работников и обучающихся хранятся в закрытых шкафах, ящиках, сейфах с ограниченным доступом лиц к данной информации. Компьютеры с персональными данными защищены секретным паролем, используются системы паролей при работе в сети (портале), обеспечено ограничение доступа к компьютерной технике для определенных категорий работников. Имеется «тревожная кнопка» - экстренный вызов полиции с использованием GSM- системы вневедомственной охраны в случае угрозы имущественной безопасности, охрану осуществляет ФГКУ «Управление вневедомственной охраны Министерства внутренних дел по КБР», обеспечена пожарная безопасность с системой оповещения. Кабинет, в котором расположены технические средства ИСПДн, оборудован пожарной сигнализацией. Входная дверь оборудована металлической решеткой с механическим замком, обеспечивающим надёжное закрытие в нерабочее время.

Хранение ПДн сотрудников осуществляется в сейфе, расположенном в кабинете директора.

6. Принципы модели угроз

В основе Модели угроз лежат следующие общие принципы:

– безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью СЗПДн;

– при формировании Модели угроз необходимо учитывать, как угрозы, осуществление которых нарушает безопасность ПДн (далее – прямые угрозы), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы);

– ПДн обрабатываются и хранятся в ИСПДн с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы ПДн;

– СЗПДн не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий;

– нарушитель может действовать на различных этапах жизненного цикла ИСПДн.

7. Модель нарушителя безопасности персональных данных

Модель вероятного нарушителя включает:

– описание возможных нарушителей;

– предположения об имеющейся у нарушителя информации об объектах атак;

– предположения об имеющихся у нарушителя средствах атак;

– описание объектов и целей атак;

– описание каналов атак.

7.1. Классификация вероятного нарушителя безопасности ИСПДн.

Потенциальными нарушителями безопасности ИСПДн МОДО ЦДО могут быть:

– внешние нарушители, осуществляющие атаки из-за пределов КЗ ИСПДн;

– внутренние нарушители, осуществляющие атаки, находясь в пределах КЗ ИСПДн.

Внешний нарушитель имеет следующие возможности:

– осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

– осуществлять деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ИСПДн и контролю порядка проведения работ.

Таблица 3 – Классификация нарушителей ИСПДн

Категория нарушителя	Описание нарушителя	Потенциальный нарушитель в ИСПДн
Н0	К категории Н0 относятся, лица не имеющие санкционированный доступ к ИСПДн. Лицо этой категории, может: – осуществлять НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок; – осуществлять НСД через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ;	Лица, не имеющие санкционированный доступ к ИСПДн, осуществляющие атаки из-за пределов КЗ. К данным лицам относятся: – посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке; – криминальные структуры.
Н1	К категории Н1 относятся, лица не имеющие санкционированный доступ к ИСПДн. Лица этой категории обладают всеми возможностями лиц категории Н0 и дополнительно им могут быть известны, полученные в рамках предоставленных полномочий, а также в результате наблюдений сведения о мерах защиты применяемых в ИСПДн.	Лица, не имеющие санкционированный доступ к ИСПДн, осуществляющие атаки из-за пределов КЗ ИСПДн, обладающие сведениями о мерах защиты объектов, в которых размещены ресурсы ИСПДн. К данным лицам относятся сотрудники МОДО ЦДО, не допущенные в КЗ ИСПДн, а также бывшие сотрудники МОДО ЦДО.
Н2	К категории Н2 относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн. Лицо этой категории, может: – иметь доступ к фрагментам информации, содержащей ПДн; – располагать именами и вести выявление паролей зарегистрированных пользователей; – изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники МОДО ЦДО, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам ИСПДн, но имеющие санкционированный доступ в КЗ, в том числе энергетики, сантехники, уборщицы, дежурные и другие лица, обеспечивающие нормальное функционирование организации.
Н3	К категории Н3 относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места. Лицо этой категории: – обладает всеми возможностями лиц категории Н2; – знает, по меньшей мере, одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн; – располагает конфиденциальными данными, к которым имеет доступ. Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.	Сотрудники МОДО ЦДО, являющиеся зарегистрированными пользователями ИСПДн, имеющие право доступа к ресурсам ИСПДн для выполнения своих должностных обязанностей.

Категория нарушителя	Описание нарушителя	Потенциальный нарушитель в ИСПДн
Н4	К категории Н4 относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн. Лицо этой категории: – обладает всеми возможностями лиц категории Н3; – обладает полной информацией об ИСПДн; – обладает полной информацией о системном и прикладном ПО 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. – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Системный администратор выполняет конфигурирование и управление ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта, за соблюдение правил разграничения доступа, за смену паролей., за архивацию и защиту от НСД.	Сотрудники МОДО ЦДО с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа.
Н5	К категории Н5 относятся программисты-разработчики (поставщики) прикладного ПО. Лицо этой категории: – обладает информацией об алгоритмах и программах обработки информации в ИСПДн; – обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения.	Программисты-разработчики прикладного ПО применяемого в ИСПДн, но не имеющие санкционированный доступ к ресурсам ИСПДн.
Н6	К категории Н6 относятся лица, обладающие возможностью: – создания способов, подготовки и проведения атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО; – проведения работ по созданию способов и средств атак в научно-исследовательских центрах; – располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СЗИ; – располагать всеми аппаратными компонентами СЗИ.	К типу нарушителей Н6 можно отнести группы специалистов по разработке и использованию специальных средств эксплуатации уязвимостей.

Обоснование перечня лиц, которые не рассматриваются в качестве потенциальных нарушителей, приведено в таблице 4.

Таблица 4 – Обоснование перечня лиц, которые не рассматриваются в качестве потенциальных нарушителей

Обоснование исключения лиц из числа потенциальных нарушителей	**Отметка об исключении лиц из групп потенциальных нарушителей**						
	Н0	**Н1**	**Н2**	**Н3**	**Н4**	**Н5**	**Н6**
Лица, отнесённые к категории нарушителей Н2, имеющие санкционированный доступ в КЗ, либо являются доверенными, либо их действия контролируется пользователем и (или) администратором ИСПДн.			+	+			
Лица, отнесённые к категории нарушителей Н3, в рамках выполнения своих функциональных обязанностей имеют возможность непосредственного доступа к ПДн, обрабатываемым в ИСПДн, и поэтому проведение атак с их стороны бессмысленно.				+			
Функции лиц, отнесённых к категории нарушителей Н4, выполняют лица, которые осуществляют техническое обслуживание как общесистемных средств ИСПДн, так и СЗИ, включая их настройку, конфигурирование и распределение паролей и ключевой документации между остальными пользователями. Лица, отнесённые к категориям нарушителей Н4, назначаются из числа особо проверенных ответственных и доверенных лиц. Эффективность всей системы безопасности ПДн зависит от адекватности действий данных лиц. Поэтому устанавливать систему защиты от них было бы нецелесообразно в связи с её беспрецедентной сложностью и низкой эффективностью (исходя из соображений, что если кто-то из этих лиц преднамеренно задумает нарушить безопасность ПДн, то предупредить реализацию такой угрозы можно только в комплексе со специальными мероприятиями, сложность которых несоразмерна с более простыми возможностями привилегированных лиц, обойти установленные для них ограничения)					+		
Лица, отнесённые к категориям нарушителей Н5, не имеют санкционированный доступ в ИСПДн, их действия контролируются администратором ИСПДн. Работы данной группой нарушителя осуществляются на основании договоров и соглашений, которые предусматривают ответственность за утечку конфиденциальной информации.						+	
Предполагается, что для категорий нарушителей Н6 проведение атак является средством менее предпочтительным, чем средства, основанные на агентурных методах, которые они предпринимают в целях получения ПДн о конкретно интересующем их лице, а не по всей базе ПДн, обрабатываемых в ИСПДн.							+

Обоснование исключения лиц из числа потенциальных нарушителей	Отметка об исключении лиц из групп потенциальных нарушителей						
	H0	H1	H2	H3	H4	H5	H6
Вывод	-	-	+	+	+	+	+

В соответствии с проведённым анализом потенциальных нарушителей в ИСПДн устанавливаются следующие категории нарушителей:

– внешние нарушители H0 и H1.

Различают высокий, средний и низкий потенциалы нарушителя.

Высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.

Средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей.

Низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Предполагается, что внешний нарушитель может обладать низким и средним потенциалом.

8. Определение класса средств криптографической защиты информации

Шифровальные (криптографические) средства: не используются.

9. Определение актуальных угроз безопасности персональных данных в информационной системе персональных данных

Актуальные УБПДн определяются в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных», утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России.

Для выявления УБПДн, актуальных для ИСПДн, оцениваются два показателя:

– уровень исходной защищенности ИСПДн;

– частота (вероятность) реализации рассматриваемой угрозы.

9.1. Уровень исходной защищённости информационной системы персональных данных

Результаты анализа исходной защищенности ИСПДн приведены в таблице 5.

Таблица 5 – Анализ исходной защищенности ИСПДн

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:			
запись, удаление, сортировка		+	
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 данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации		+	
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая часть ПДн		+	
Характеристики ИСПДн	**29%**	**71%**	**0%**

Таким образом, ИСПДн имеет средний (Y_1=5) уровень исходной защищённости.

9.2. Частота (вероятность) реализации угроз безопасности персональных данных

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы равен двум, т.е. объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y_2 = 2 низкая вероятность).

Коэффициент реализуемости угрозы Y будет определяться исходя из исходного уровня защищенности ИСПДн и вероятности реализации УБПДн соотношением:

$$Y = (Y_1+Y_2)/20$$

$$Y = (5+2)/20 = 0,35$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы. Возможность реализации угрозы признается средней т.к. $0,3 < Y \le 0,6$.

Показатель опасности угрозы низкий (реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных).

9.3. Определение актуальности угроз безопасности персональных данных

Угрозы безопасности ПДн относятся к неактуальным, исходя из возможности реализации угроз и показателя опасности угрозы, в соответствии с таблицей 6.

Таблица 6 – Правила отнесения УБПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая опасность	**Средняя опасность**	**Высокая опасность**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	**Неактуальная**	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

10. Заключение

Модель угроз МОДО ЦДО содержит следующие возможные УБПДн для ИСПДн:

– УБИ.008: Угроза восстановления аутентификационной информации;

– УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути;

– УБИ.022: Угроза избыточного выделения оперативной памяти;

– УБИ.031: Угроза использования механизмов авторизации для повышения привилегий;

– УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными;

– УБИ.063: Угроза некорректного использования функционала программного обеспечения;

– УБИ.069: Угроза неправомерных действий в каналах связи;

– УБИ.074: Угроза несанкционированного доступа к аутентификационной информации;

– УБИ.086: Угроза несанкционированного изменения аутентификационной информации;

– УБИ.088: Угроза несанкционированного копирования защищаемой информации;

– УБИ.089: Угроза несанкционированного редактирования реестра;

– УБИ.090: Угроза несанкционированного создания учётной записи пользователя;

– УБИ.091: Угроза несанкционированного удаления защищаемой

информации;

– УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

– УБИ.099: Угроза обнаружения хостов;

– УБИ.104: Угроза определения топологии вычислительной сети;

– УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации;

– УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети;

– УБИ.121: Угроза повреждения системного реестра;

– УБИ.127: Угроза подмены действия пользователя путём обмана;

– УБИ.132: Угроза получения предварительной информации об объекте защиты;

– УБИ.139: Угроза преодоления физической защиты;

– УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.152: Угроза удаления аутентификационной информации;

– УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.158: Угроза форматирования носителей информации;

– УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.172: Угроза распространения почтовых червей;

– УБИ.186: Угрозы внедрения по сети вредоносных программ;

– УБИ.195: Угрозы удаленного запуска приложений.

РАЗРАБОТАНА

Должность исполнителя	**Фамилия, имя, отчество**	**Подпись**	**Дата**
Методист по ПО	Цаголов А.Р.		
Методист по УВР	Хачатурян А.Р.		