

МИНИСТЕРСТВО КУЛЬТУРЫ РЕСПУБЛИКИ КРЫМ

Государственное бюджетное учреждение культуры Республики Крым
«Крымская республиканская библиотека для молодежи»
(ГБУК РК КРБДМ)

ПРИКАЗ

08 апреля 2024 г.

№ 43

г. Симферополь

Об утверждении Модели
угроз ГБУК КРБДМ

В целях выполнения требований Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ, Постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119, Приказа ФСБ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10 июля 2014 года № 378,

ПРИКАЗЫВАЮ:

1. Утвердить Модель угроз Государственного бюджетного учреждения культуры Республики Крым «Крымская республиканская библиотека для молодежи» (Приложение № 1).

2. Системному администратору разместить Модель угроз ГБУК КРБДМ на официальном сайте учреждения.

3. Контроль за выполнением настоящего приказа оставляю за собой.

Директор



А.А. Подшивалова

С приказом ознакомлен:

Полянчук Д.М.



«08» апреля 2024 г.

УТВЕРЖДЕНО
приказом от 08.04.2024 г. № 43

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ
ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ
ДАННЫХ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ
КУЛЬТУРЫ РЕСПУБЛИКИ КРЫМ
«КРЫМСКАЯ РЕСПУБЛИКАНСКАЯ БИБЛИОТЕКА ДЛЯ МОЛОДЁЖИ»**

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИС – информационная система
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СВТ – средства вычислительной техники
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СКЗИ – средства криптографической защиты информации
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

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

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.

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

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.

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

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

таких процессов и методов.

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

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних 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 распространения 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.

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

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.

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

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

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, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

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

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

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.

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

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

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

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

Угрозы безопасности 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 – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты информации и персональных данных:

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

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

3. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные Постановлением Правительства Российской Федерации № 1119 от 1 ноября 2012 года;

4. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные Приказом ФСТЭК России № 17 от 11 февраля 2013 года;

5. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден Приказом ФСТЭК России № 21 от 18 февраля 2013 года;

6. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных, утвержденная 14 февраля 2008 года заместителем директора ФСТЭК России;

7. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных, утвержденная 15 февраля 2008 года заместителем директора ФСТЭК России;

8. Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru);

9. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432;

10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержден Приказом ФСБ России от 10 июля 2014 года № 378.

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России, регламентирующих порядок обеспечения безопасности ПДн.

Настоящая Модель угроз содержит систематизированный перечень угроз безопасности ПДн и иной защищаемой информации при их обработке в информационной системе Государственного бюджетного учреждения культуры Республики Крым «Крымская республиканская библиотека для молодёжи» (далее – ГБУК КРБДМ). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, создающими условия (предпосылки) для нарушения безопасности ПДн и иной защищаемой информации, которые ведут к ущербу жизненно важных интересам личности и общества.

Модель угроз определяет актуальные угрозы для ИСПДн ГБУК КРБДМ.

Модель угроз содержит данные по угрозам безопасности ПДн и иной защищаемой информации, обрабатываемых в ГБУК КРБДМ, связанным:

- с перехватом ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн ГБУК КРБДМ с целью изменения, копирования, неправомерного распространения уничтожения или блокирования ПДн, с использованием программных и программно-аппаратных средств.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц ГБУК КРБДМ – администраторов ИСПДн.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн ГБУК КРБДМ от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ГБУК КРБДМ, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением четвертого уровня защищенности персональных данных и третьего класса защищенности ГБУК КРБДМ.

В Модели угроз дано обобщённое описание ИСПДн ГБУК КРБДМ как объекта защиты, возможных источников УБПДн, основных классов уязвимостей информационной системы, возможных видов неправомерных действий в отношении ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ГБУК КРБДМ, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн ГБУК КРБДМ. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в Базовую модель угроз безопасности персональных данных ФСТЭК и Банк данных угроз безопасности информации ФСТЭК России. Кроме того, Модель угроз может быть пересмотрена по решению оператора (ГБУК КРБДМ) на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений информационной системы, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

ПРИНЦИПЫ МОДЕЛИ УГРОЗ

В основе Модели угроз лежат следующие общие принципы:

1. Безопасность персональных данных и иной защищаемой информации при их обработке в информационных системах обеспечивается с помощью системы защиты информации в ГБУК КРБДМ.

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

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. Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

5. Система защиты информации ИСПДн ГБУК КРБДМ (в том числе и СКЗИ) не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (система защиты информации не предназначена для защиты информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

6. Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

7. Криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ.

8. СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

9. Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

МОДЕЛЬ УГРОЗ ГБУК КРБДМ

Общие сведения об информационной системе

Назначение ИС – автоматизация деятельности учреждений культуры.

Оператор ИС – юридическое лицо, Государственное бюджетное учреждение культуры Республики Крым «Крымская республиканская библиотека для молодёжи.

ГБУК КРБДМ охраняется частной охранной организацией.

В ИСПДн ГБУК КРБДМ необходимо обеспечить конфиденциальность, целостность и доступность персональных данных.

В ИСПДн ГБУК КРБДМ обрабатываются специальные категории персональных данных менее 100 000 субъектов.

Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных

В ИСПДн ГБУК КРБДМ существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ. К таким угрозам относятся угрозы, связанные с передачей персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

Для ИСПДн ГБУК КРБДМ достаточным классом защиты является КС1. Данный класс защиты предназначен для защиты информации, требующей обычной степени конфиденциальности и целостности. КС1 гарантирует защиту от типичных методов атак, используемых большинством злоумышленников. Классом КС1 защищаются данные, которые не содержат государственной тайны или коммерческой тайны, а также персональные данные

Дополнительные объекты защиты

В ИСПДн ГБУК КРБДМ к объектам защиты дополнительно относятся:

1. применяемые в ИСПДн ГБУК КРБДМ СКЗИ;
2. среда функционирования криптосредства (СФК);
3. информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
4. документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФК;
5. носители защищаемой информации, используемые в ИСПДн ГБУК КРБДМ в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
6. используемые каналы (линии) связи;
7. помещения, в которых находятся ресурсы ИСПДн ГБУК КРБДМ, имеющие отношение к криптографической защите персональных данных.

Тип ИСПДн

Таблица 1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Типовая информационная система
Структура информационной системы	Локальная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Подключена
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Права доступа разграничены исходя из роли пользователя в системе
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и (или) доступности

Исходя из параметров ИСПДн, текущую информационную систему персональных данных можно отнести к локальной информационной системе (ЛИС) II типа.

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.

Исходный уровень защищенности ИСПДн

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

ИСПДн ГБУК КРБДМ имеет следующие технические и эксплуатационные характеристики:

1. Территориальное размещение ИСПДн ГБУК КРБДМ - локальная ИСПДн ГБУК КРБДМ, развернута в пределах одного здания. Уровень защищенности – **высокий**.

2. Наличие соединения с сетями связи общего пользования – ИСПДн ГБУК КРБДМ, имеет одноточечный выход в сеть общего пользования. Уровень защищенности – **средний**.

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

4. Разграничение доступа к персональным данным – к ИСПДн ГБУК КРБДМ имеет доступ определенный перечень сотрудников организации, являющиеся администратором, либо пользователем ИСПДн ГБУК КРБДМ. Уровень защищенности – **средний**.

5. Наличие соединений с другими базами персональных данных иных информационных систем – ИСПДн ГБУК КРБДМ используется единая база ПДн, принадлежащая организации (оператору) данной информационной системы. Уровень защищенности – **высокий**.

6. Уровень обобщения (обезличивания) персональных данных – ИСПДн ГБУК КРБДМ, в которой предоставляемые пользователю данные являются обезличенными

(т.е. не присутствует информация, позволяющая идентифицировать субъекта ПДн).
Уровень защищенности – **средний**.

7. Объем персональных данных, которые предоставляются сторонним субъектам без предварительной обработки – ИСПДн ГБУК КРБДМ, не предоставляет никакой информации. Уровень защищенности – **высокий**.

Определение исходного уровня защищенности:

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

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

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

Таблица 2 – Уровни защищённости

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений
1	Высокий	3	43%
2	Средний	3	43%
3	Низкий	1	14%

В соответствии с полученными данными устанавливается **средний показатель исходной защищенности**, значение коэффициента $Y_1=5$.

ПОЛЬЗОВАТЕЛИ ИСПДн ГБУК КРБДМ

В Государственном бюджетном учреждении культуры Республики Крым «Крымская республиканская библиотека для молодёжи» обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице 3.

Таблица 3 – Распределение ролей

Группа	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	<p>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.</p>	<p>сбор систематизация запись накопление извлечение хранение уточнение использование блокировка удаление уничтожение</p>
Администратор безопасности	<p>Обладает правами Администратора ИСПДн. 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).</p>	<p>сбор систематизация запись накопление извлечение хранение уточнение использование блокировка удаление уничтожение</p>
Пользователь ИСПДн	<p>Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.</p>	<p>сбор систематизация запись накопление извлечение передача хранение уточнение использование обезличивание удаление уничтожение</p>

Предоставление или прекращение доступа к ИСПДн осуществляется в соответствии с приказом о назначении на должность или приказом об увольнении.

МОДЕЛЬ НАРУШИТЕЛЯ

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения безопасности информационной системы.

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

Внешние нарушители – физические лица, не имеющие права пребывания на территории учреждения, в пределах которой размещается оборудование ИСПДн ГБУК КРБДМ;

Внутренние нарушители – физические лица, имеющие право пребывания на территории учреждения, в пределах которой размещается оборудование ИСПДн ГБУК КРБДМ.

Внешний нарушитель

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

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн ГБУК КРБДМ, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

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

Система разграничения доступа ИСПДн ГБУК КРБДМ обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн ГБУК КРБДМ в соответствии с принятой Инструкцией пользователя информационной системы персональных данных Государственного бюджетного учреждения культуры Республики Крым «Крымская республиканская библиотека для молодежи».

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз информационной безопасности, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, 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, не 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 информационные и управляющие интерфейсы средств вычислительной техники;

- средств воздействия на источники и через цепи электропитания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

К внутренним нарушителям могут относиться:

- администратор безопасности ИСПДн ГБУК КРБДМ (категория I);
- администраторы подсистем или баз данных ИСПДн ГБУК КРБДМ (категория II);
- пользователи ИСПДн ГБУК КРБДМ (категория III);
- пользователи, являющиеся внешними по отношению к конкретной автоматизированной системе (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн ГБУК КРБДМ, но не имеющие права доступа к ним (категория VI);
- прочий персонал (рабочий, уборщик помещений и т.п.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн ГБУК КРБДМ, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн ГБУК КРБДМ (категория VIII).

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

На лиц категорий I-II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн ГБУК КРБДМ для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн ГБУК КРБДМ. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн ГБУК КРБДМ, а также к техническим и программным средствам ИСПДн ГБУК КРБДМ, включая средства защиты, используемые в конкретных автоматизированных системах, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн ГБУК КРБДМ 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 информационной безопасности. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников (сети Интернет)).

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

Предполагается, что в число лиц категорий I-II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

В качестве основных уровней знаний нарушителей об автоматизированной системе можно выделить следующие:

- общая информация – информации о назначении и общих характеристиках ИСПДн ГБУК КРБДМ;
- эксплуатационная информация – информация, полученная из эксплуатационной документации;

- чувствительная информация – информация, дополняющая эксплуатационную информацию о ИСПДн ГБУК КРБДМ (например, сведения из проектной документации ИСПДн ГБУК КРБДМ).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн ГБУК КРБДМ;
- сведения об информационных ресурсах ИСПДн ГБУК КРБДМ: 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 ГБУК КРБДМ;
- данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн ГБУК КРБДМ;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в автоматизированной информационной системе (АИС), к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VIII обладают чувствительной информацией о ИСПДн ГБУК КРБДМ и функционально ориентированных автоматизированных систем, включая информацию об уязвимостях технических и программных средств ИСПДн ГБУК КРБДМ. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн ГБУК КРБДМ в момент обработки ПДн с использованием средств защищаемой информации.

Таким образом, наиболее информированными об ИСПДн ГБУК КРБДМ являются лица категории III и лица категории VIII.

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.

Предположения об имеющихся у нарушителя средствах реализации угроз:

- аппаратные компоненты средства защиты ПДн (СЗПДн);
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Нарушители согласно банку данных угроз ФСТЭК России

Дополнительно в банке данных угроз ФСТЭК России определены три типа внешних и внутренних нарушителей – с низким потенциалом, со средним потенциалом и с высоким потенциалом.

Нарушители с низким потенциалом имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Также такие нарушители имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушители со средним потенциалом обладают всеми возможностями нарушителей с низким потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушители с высоким потенциалом обладают всеми возможностями нарушителей с низким и средним потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

Для ИСПДн ГБУК КРБДМ определен нарушитель с **низким** потенциалом.

ВЕРОЯТНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИСПДн ГБУК КРБДМ

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 учреждения 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 источником ПДн, что создает необходимые условия для нарушения безопасности ПДн.

Основными элементами канала реализации УБПДн являются:

- источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;
- среда распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программное обеспечение 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.

Классификация уязвимостей ИСПДн

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

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 расходом ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- 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).

Перечень возможных УБПДн

Для ИСПДн ГБУК КРБДМ можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам.
 - 1.1. Угрозы утечки акустической информации.
 - 1.2. Угрозы утечки видовой информации.
 - 1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации.
 - 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.
 - 2.1.1. Кража ПЭВМ;
 - 2.1.2. Кража носителей информации;
 - 2.1.3. Кража ключей и атрибутов доступа;
 - 2.1.4. Кража, изменение, уничтожение информации;
 - 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи;
 - 2.1.6. Несанкционированное отключение средств защиты.
 - 2.2. Угрозы хищения, несанкционированного изменения или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств.
 - 2.2.1. Действия вредоносных программ (вирусов);
 - 2.2.2. Недекларированные возможности системного ПО и ПО для обработки ПДн;

- 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей.
- 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в программном обеспечении, а также от угроз технического и стихийного характера.
 - 2.3.1. Утрата ключей и атрибутов доступа;
 - 2.3.2. Непреднамеренное изменение и уничтожение информации сотрудниками;
 - 2.3.3. Непреднамеренное отключение средств защиты;
 - 2.3.4. Выход из строя аппаратно-программных средств;
 - 2.3.5. Сбой системы электроснабжения;
 - 2.3.6. Стихийное бедствие.
- 2.4. Угрозы преднамеренных действий внутренних нарушителей.
 - 2.4.1. Доступ к информации, ее изменение и уничтожение лицами, не допущенными к обработке информации;
 - 2.4.2. Разглашение информации третьим лицам, ее изменение и уничтожение сотрудниками, допущенными к обработке информации.
- 2.5. Угрозы несанкционированного доступа по каналам связи.
 - 2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации.
 - 2.5.1.1. Перехват за пределами контролируемой зоны;
 - 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;
 - 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.
 - 2.5.2. Угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и т.д.
 - 2.5.3. Угрозы выявления паролей по сети.
 - 2.5.4. Угрозы навязывание ложного маршрута сети.
 - 2.5.5. Угрозы подмены доверенного объекта в сети.
 - 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.
 - 2.5.7. Угрозы типа «Отказ в обслуживании».
 - 2.5.8. Угрозы удаленного запуска приложений.
 - 2.5.9. Угрозы внедрения по сети вредоносных программ.

Вероятность реализации УБПДн

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

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по четырем 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 ($Y_2 = 10$).

УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Угрозы утечки акустической (речевой) информации

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

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

Вероятность реализации угрозы – **маловероятна**.

Угрозы утечки видовой информации

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

На окнах учреждения используются жалюзи и занавески. Доступ посторонних лиц в помещения, в которых производится обработка ПДн, ограничен.

Вероятность реализации угрозы – **маловероятна**.

Угрозы утечки информации по каналам ПЭМИН

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

Угроза утечки информации, содержащей ПДн, по каналу ПЭМИН возможна, за счет перехвата техническими средствами разведки за пределами контролируемой зоны ПЭМИН, возникающих при обработке ПДн средствами вычислительной техники ИСПДн.

Элементы ИСПДн экранируются несколькими несущими стенами. Интересующий потенциального злоумышленника сигнал маскируется с множеством других паразитных сигналов, не содержащих элементов входящих в ИСПДн.

Вероятность реализации угрозы – **маловероятна**.

Угрозы несанкционированного доступа к информации

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

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

Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн

Кража ПЭВМ осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В ГБУК КРБДМ введен контроль доступа. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на посту охраны, выдача ключей ответственным сотрудникам

организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Вероятность реализации угрозы – **маловероятна.**

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

В учреждении введен контроль доступа. Съемные носители информации хранятся в специально отведенных помещениях, в сейфах. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на посту охраны, выдача ключей ответственным сотрудникам организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Доступ к техническим средствам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора. Переносные компьютеры для обработки ПДн в ИСПДн не используются.

Вероятность реализации угрозы – **маловероятна.**

Кража ключей и атрибутов доступа осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где происходит работа пользователей.

В учреждении введен контроль доступа. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на посту охраны, выдача ключей ответственным сотрудникам организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Вероятность реализации угрозы – **маловероятна.**

Кража, изменение, уничтожение информации осуществляется путём НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В учреждении введен контроль доступа. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на посту охраны, выдача ключей ответственным сотрудникам организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Вероятность реализации угрозы – **маловероятна.**

Вывод из строя узлов ПЭВМ и каналов связи осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн и проходят каналы связи.

В учреждении введен контроль доступа. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на посту охраны, выдача ключей ответственным сотрудникам организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Вероятность реализации угрозы – **маловероятна.**

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

В Учреждении введен контроль доступа. Ключи от помещений, где хранятся и обрабатываются ПДн, а также помещения, где расположено серверное оборудование учреждения хранятся на пульте охраны, выдача ключей ответственным сотрудникам организована строго по Журналу учета ключей и приема помещений в ГБУК КРБДМ и в соответствии с Порядком доступа в помещения, в которых ведется обработка персональных данных ГБУК КРБДМ.

Возможность отключения или изменения настроек СЗИ пользователем запрещена. Настройка средств разграничения доступа к ресурсам ИСПДн производится системным администратором.

Вероятность реализации угрозы – **маловероятна**.

Угрозы хищения, несанкционированной модификации, удаления или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств

Одним из способов воздействия на ИСПДн является программно-математическое воздействие с помощью вредоносных программ (вирусов). Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют стороннее самостоятельное ПО, которое способно выполнять следующие функции:

- 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 (копирование, уничтожение, блокирование 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 учреждении на всех элементах ИСПДн установлена лицензионная отечественная антивирусная система Dr. Web, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая**.

Недекларированные возможности системного ПО и ПО для обработки персональных данных – это функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Вероятность реализации угрозы повышается:

- при увеличении элементов, в том числе программного обеспечения, ИСПДн;
- при увеличении числа функциональных связей между элементами;
- наличии подключения к сетям общего доступа и (или) международного обмена.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 4.

Таблица 4

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	низкая	2
Распределенная ИС II типа	низкая	2

В случае если в обработке персональных данных участвует ПО собственной разработки или стандартное ПО, доработанное под нужды учреждения, то следует повысить значение вероятности реализации угрозы:

- для всех типов ИСПДн, кроме Автономная ИС I типа, на порядок;
- для Распределенной ИС II типа на два порядка.

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **низкая**.

Угроза несанкционированной установки ПО, не связанного с исполнением служебных обязанностей внутренними нарушителями может привести к нарушению конфиденциальности, целостности и доступности ИСПДн или ее элементов.

В учреждении введено разграничение прав пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы – **маловероятна**.

Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в программном обеспечении, а также от угроз технического и стихийного характера.

Утрата ключей и атрибутов доступа может произойти из-за человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, периодически не изменяют и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В ГБУК КРБДМ введена парольная политика, предусматривающая сложность пароля и периодическую его смену, запрещена запись паролей пользователю на бумажные носители. Пользователи проинструктированы о парольной политике и о действиях в случае утраты или компрометации паролей.

Вероятность реализации угрозы – **маловероятна**.

Непреднамеренное изменение и уничтожение информации может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают правила работы с конфиденциальной информацией.

Перед началом работы каждый пользователь изучает локальные документы ГБУК КРБДМ, регламентирующие работу сотрудников с персональными данными.

В учреждении осуществляется резервное копирование обрабатываемых ПДн на носители, которые хранятся в сейфе ответственного лица.

Вероятность реализации угрозы – **маловероятна**.

Непреднамеренное отключение средств защиты может случиться из-за человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В ГБУК КРБДМ осуществляется разграничение доступа к настройкам режимов средств защиты.

Вероятность реализации угрозы - **маловероятна**.

Выход из строя аппаратно-программных средств возможен вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В ГБУК КРБДМ осуществляется резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

Сбой системы электроснабжения возможен вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В ГБУК КРБДМ ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляется резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

Стихийное бедствие возможно вследствие несоблюдения мер пожарной безопасности.

В ГБУК КРБДМ установлена пожарная сигнализация, в наличии необходимое количество противопожарного инвентаря (в т. ч. огнетушители) пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна**.

Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, её изменение и уничтожение лицами, не допущенными к ее обработке, возможен путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В ГБУК КРБДМ введен контроль доступа в контролируемую зону, помещения закрываются на ключ.

Вероятность реализации угрозы – **маловероятна**.

Разглашение информации третьим лицам сотрудниками, допущенными к ее обработке возможно за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В ГБУК КРБДМ пользователи осведомлены о порядке работы с персональными данными, а также на них возложена обязанность о неразглашении персональных данных, в соответствии с Обязательством о неразглашении персональных данных ГБУК КРБДМ.

Вероятность реализации угрозы – **маловероятна**.

Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн ГБУК КРБДМ можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и т.д.;
- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

Угроза «Анализ сетевого трафика» 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 серверами, 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 серверам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, изменения и т.п.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 5.

Таблица 5

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **низкая**.

Перехват в пределах контролируемой зоны внешними нарушителями неоснователен, т.к. в ГБУК КРБДМ введен контроль доступа в контролируемую зону, помещения закрываются на ключ.

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями неоснователен, т.к. в ГБУК КРБДМ введен контроль доступа в контролируемую зону, помещения закрываются на ключ.

Вероятность реализации угрозы – **маловероятна**.

Угроза «Сканирование сети» в локальной сети возможна в случае передачи запросов сетевым службам серверов ИСПДн и анализе ответов от них. Цель угрозы – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей. Реализация данной угрозы в локальной сети наиболее вероятна со стороны внутреннего нарушителя.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 6.

Таблица 6

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Сетевое оборудование, применяемое в ИСПДн ГБУК КРБДМ, размещается в служебных помещениях в пределах учреждения. Доступ в помещение, где расположено серверное оборудование, элементы ИСПДн и помещения узлов связи разрешено только ограниченному кругу лиц.

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **маловероятна**.

Угроза выявления паролей 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 серверу путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на сервере изменить пароль доступа.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 7.

Таблица 7

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

Сетевое оборудование, применяемое в ИСПДн ГБУК КРБДМ, размещается в служебных помещениях в пределах учреждения. Доступ в помещение, где расположено серверное оборудование, элементы ИСПДн и помещения узлов связи разрешено только ограниченному кругу лиц.

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **маловероятна.**

Угроза навязывания ложного маршрута сети реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на сервер или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна.**

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 8.

Таблица 8

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **маловероятна**.

Угроза подмены доверенного объекта эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации серверов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн – цели угроз.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 9.

Таблица 9

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).

Вероятность реализации угрозы – **маловероятна**.

Угроза внедрения ложного объекта сети основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях NovellNetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 10.

Таблица 10

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	маловероятная	0
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	низкая	2

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **маловероятна**.

Угрозы типа «Отказ в обслуживании» 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 (Pingflooding), 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 техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, 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 «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления 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.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 11.

Таблица 11

Тип ИСПДн	Вероятность реализации угрозы	Коэфф. вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	маловероятная	0
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	маловероятная	0
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	маловероятная	0
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	низкая	2
Распределенная ИС II типа	низкая	2

Серверное оборудование ИСПДн ГБУК КРБДМ защищено межсетевым экраном. Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа). Вероятность реализации угрозы – **низкая**.

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

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 виде 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.

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например,

«троянскими» программами типа Back.Orifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 12.

Таблица 12

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа). Вероятность реализации угрозы – **низкая**.

Угроза внедрения по сети вредоносных программ возможна при внедрении по сети. К таким угрозам 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, спровоцировать пользователя на запуск 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.

Если в учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – **маловероятна**.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 13.

Таблица 13

Тип ИСПДн	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
Автономная ИС I типа	маловероятная	0
Автономная ИС II типа	низкая	2
Автономная ИС III типа	маловероятная	0
Автономная ИС IV типа	низкая	2
Автономная ИС V типа	маловероятная	0
Автономная ИС VI типа	низкая	2
ЛИС I типа	маловероятная	0
ЛИС II типа	низкая	2
Распределенная ИС I типа	маловероятная	0
Распределенная ИС II типа	средняя	5

Для ИСПДн ГБУК КРБДМ установлен тип Локальная ИС II типа (ЛИС II типа).
Вероятность реализации угрозы – **низкая**.

РЕАЛИЗУЕМОСТЬ ПОТЕНЦИАЛЬНЫХ УГРОЗ

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$

Оценка реализуемости УБПДн представлена в таблице 14.

Таблица 14 – Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
Угрозы от утечки по техническим каналам		
Угрозы утечки акустической информации	0,25	маловероятная
Угрозы утечки видовой информации	0,25	маловероятная
Угрозы утечки информации по каналам ПЭМИН	0,25	маловероятная
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
Кража ПЭВМ	0,25	маловероятная
Кража носителей информации	0,25	маловероятная
Кража ключей и атрибутов доступа	0,25	маловероятная
Кража, изменение, уничтожение информации	0,25	маловероятная
Вывод из строя узлов ПЭВМ, каналов связи	0,25	маловероятная
Несанкционированное отключение средств защиты	0,25	маловероятная

Угрозы хищения, несанкционированной модификации или блокирования информации засчет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств		
Действия вредоносных программ (вирусов)	0,35	низкая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,35	низкая
Установка ПО, не связанного с исполнением служебных обязанностей	0,25	маловероятная
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в программном обеспечении, атаке от угроз технического и стихийного характера		
Утрата ключей и атрибутов доступа	0,25	маловероятная
Непреднамеренное изменение и уничтожение информации сотрудниками	0,25	маловероятная
Непреднамеренное отключение средств защиты	0,25	маловероятная
Выход из строя аппаратно-программных средств	0,25	маловероятная
Сбой системы электроснабжения	0,25	маловероятная
Стихийное бедствие	0,25	маловероятная
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, ее изменение и уничтожение лицами, не допущенными к ее обработке	0,25	маловероятная
Разглашение информации третьим лицам, изменение и уничтожение информации сотрудниками допущенными к ее обработке	0,25	маловероятная
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	0,25	низкая
Перехват за пределами контролируемой зоны	0,35	низкая
Перехват в пределах контролируемой зоны внешними нарушителями	0,25	маловероятная
Перехват в пределах контролируемой зоны внутренними нарушителями	0,25	маловероятная
Угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и т.д.	0,25	маловероятная
Угрозы выявления паролей по сети	0,25	маловероятная
Угрозы навязывание ложного маршрута сети	0,25	маловероятная

Угрозы подмены доверенного объекта в сети	0,25	маловероятная
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	маловероятная
Угрозы типа «Отказ в обслуживании»	0,35	низкая
Угрозы удаленного запуска приложений	0,35	низкая
Угрозы внедрения по сети вредоносных программ	0,35	низкая

ОЦЕНКА ОПАСНОСТИ УГРОЗ

Оценка опасности угроз безопасности персональных данных в информационной системе персональных данных (ИСПДн) проведена Комиссией по защите информации включая персональные данные ГБУК КРБДМ.

Оценка опасности УБПДн 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 для ИСПДн ГБУК КРБДМ представлена таблице 15.

Таблица 15 – Опасность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
Угрозы от утечки по техническим каналам	
Угрозы утечки акустической информации	низкая
Угрозы утечки видовой информации	низкая
Угрозы утечки информации по каналам ПЭМИН	низкая
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	низкая
Кража носителей информации	низкая
Кража ключей и атрибутов доступа	низкая
Кража, изменение, уничтожение информации	низкая
Вывод из строя узлов ПЭВМ, каналов связи	низкая
Несанкционированное отключение средств защиты	низкая
Угрозы хищения, несанкционированной модификации или блокирования информации засчет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств	
Действия вредоносных программ (вирусов)	средняя
Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая
Установка ПО не связанного с исполнением служебных обязанностей	низкая
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в программном обеспечении, а также от угроз технического и стихийного характера	
Утрата ключей и атрибутов доступа	средняя
Непреднамеренное изменение и уничтожение информации сотрудниками	низкая
Непреднамеренное отключение средств защиты	низкая
Выход из строя аппаратно-программных средств	низкая
Сбой системы электроснабжения	низкая
Стихийное бедствие	низкая
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, её изменение и уничтожение лицами не допущенными к ее обработке	низкая
Разглашение информации третьим лицам, изменение и уничтожение информации сотрудниками допущенными к ее обработке	низкая
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	низкая
Перехват за пределами контролируемой зоны	низкая
Перехват в пределах контролируемой зоны внешними нарушителями	низкая
Перехват в пределах контролируемой зоны внутренними нарушителями	низкая

Угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и т.д.	низкая
Угрозы выявления паролей по сети	низкая
Угрозы навязывание ложного маршрута сети	низкая
Угрозы подмены доверенного объекта в сети	низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
Угрозы типа «Отказ в обслуживании»	низкая
Угрозы удаленного запуска приложений	низкая
Угрозы внедрения по сети вредоносных программ	средняя

ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ

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

Таблица 16 – Правила определения актуальности УБПДн

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Маловероятно	неактуальная	неактуальная	актуальная
Низкая	неактуальная	актуальная	актуальная
Средняя	актуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице 17.

Таблица 17 – Актуальность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
Угрозы от утечки по техническим каналам	
Угрозы утечки акустической информации	неактуальная
Угрозы утечки видовой информации	неактуальная
Угрозы утечки информации по каналам ПЭМИН	неактуальная
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	неактуальная
Кража носителей информации	неактуальная
Кража ключей и атрибутов доступа	неактуальная
Кражи, модификации, уничтожения информации	неактуальная
Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
Несанкционированное отключение средств защиты	неактуальная

Угрозы хищения, несанкционированной модификации или блокирования информации засчет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств	
Действия вредоносных программ (вирусов)	актуальная
Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в программном обеспечении, а также от угроз технического и стихийного характера	
Утрата ключей и атрибутов доступа	неактуальная
Непреднамеренная изменение и уничтожение информации сотрудниками	неактуальная
Непреднамеренное отключение средств защиты	неактуальная
Выход из строя аппаратно-программных средств	неактуальная
Сбой системы электроснабжения	неактуальная
Стихийное бедствие	неактуальная
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, её изменение и уничтожение лицами не допущенными к ее обработке	неактуальная
Разглашение информации третьим лицам, изменение и уничтожение информации сотрудниками допущенными к ее обработке	неактуальная
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	неактуальная
Перехват за пределами контролируемой зоны	неактуальная
Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
Перехват в пределах контролируемой зоны внутренними нарушителями	неактуальная
Угрозы сканирования, направленные на выявление типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и т.д.	неактуальная
Угрозы выявления паролей по сети	неактуальная
Угрозы навязывание ложного маршрута сети	неактуальная
Угрозы подмены доверенного объекта в сети	неактуальная
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
Угрозы типа «Отказ в обслуживании»	неактуальная
Угрозы удаленного запуска приложений	неактуальная
Угрозы внедрения по сети вредоносных программ	актуальная

В результате проделанной работы были выявлены следующие актуальные угрозы для ИСПДн ГБУК КРБДМ:

- действия вредоносных программ (вирусов);
- угрозы внедрения по сети вредоносных программ.

Для снижения опасности реализации актуальных УБПДн рекомендуется:

- проводить регулярные инструктажи с пользователями ИСПДн на предмет запрета установки сторонних аппаратных средств, подключения личных мобильных устройств и неучтённых внешних носителей;
- постоянное обновление антивирусных баз имеющегося антивирусного ПО;
- увеличение количества рабочих станций антивирусного ПО.