Приложение №1
к приказу от 21.02.2018
г. № 39-ОД

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в информационной системе персональных данных (далее – ИСПД):

1) ГИС «Электронное образование в Республике Татарстан»;
2) Свободное программное обеспечение «Барс-бюджет»;
3) Региональная информационная система ГИА;
4) ГИС «Электронный детский сад»

включает:

- описание угроз.
- оценку вероятности возникновения угроз.
- оценку реализуемости угроз.
- оценку опасности угроз.
- определение актуальности угроз.

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

1.Описание угроз и оценка вероятности их возникновения

Классификация нарушителей

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

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД.

Внешний нарушитель

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

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

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 контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПД обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПД в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПД (категория I);
- администраторы конкретных подсистем или баз данных ИСПД (категория II);

- пользователи ИСПД (категория III);

- пользователи, являющиеся внешними по отношению к конкретной автоматизированной системе (категория IV);

- лица, обладающие возможностью доступа к системе передачи данных (категория V);

- сотрудники учреждения, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПД, но не имеющие права доступа к ним (категория VI);

- обслуживающий персонал учреждения (категория VII);

- уполномоченный персонал разработчиков ИСПД, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПД (категория VIII).

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

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПД в целом, а также с применяемыми принципами и концепциями безопасности.

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

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

К лицам категорий I и II ввиду их исключительной роли в ИСПД 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 и 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.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

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

- *общая информация* – информации о назначения и общих характеристиках ИСПД;

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

- *чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПД (например, сведения из проектной документации ИСПД).

В частности, нарушитель может иметь:

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

- сведения об информационных ресурсах ИСПД: 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 ИСПД;
- данные о реализованных в программных средствах защиты информации (далее – ПСЗИ) принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПД;
- 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 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 VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПД и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПД. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПД в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ 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

Предполагается, что нарушитель имеет:

- аппаратные компоненты системы защиты персональных данных (далее – СЗПД);
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные в учреждении 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 СЗПД предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи;
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

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

Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПД, при обработке персональных данных (далее – ПД) в ИСПД, возможно при наличием функций голосового ввода ПД в ИСПД или функций воспроизведения ПД акустическими средствами ИСПД.

В ИСПД Учреждения функции голосового ввода ПД или функции воспроизведения ПД акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятна**.

Угрозы утечки видовой информации

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

В учреждении введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы – **маловероятна**.

Побочные ЭлектроМагнитные Излучения и Наводки

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН)

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

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

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

Кража персональной электронной вычислительной машины (далее - ПЭВМ.)

Угроза осуществляется путем несанкционированного доступа (далее – НСД) внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД.

В учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы – **маловероятна**.

Кража ключей и атрибутов доступа

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

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, организовано хранение ключей в сейфе и введена политика «чистого стола».

Вероятность реализации угрозы – **маловероятна**.

Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД и проходят каналы связи.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПД.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, пользователи ИСПД проинструктированы о работе с ПД.

Вероятность реализации угрозы – **маловероятна**.

Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств.

Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;

- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

- разрушать (искажать произвольным образом) код программ в оперативной памяти;

- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

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

- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В Учреждении на всех элементах ИСПД установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – **низкая**.

Недекларированные возможности системного программного обеспечения (далее – ПО) и ПО для обработки персональных данных.

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

В Учреждении нет программного обеспечения разрабатываемого собственными разработчиками/сторонними специалистами.

Вероятность реализации угрозы – **маловероятна**.

Установка ПО не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПД или ее элементов.

В Учреждении осуществляется контроль по используемому ПО, пользователи проинструктированы о политике установки ПО, утвержден перечень разрешенного ПО.

Вероятность реализации угрозы – **низкая**.

Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от стихийного характера.

Утрата ключей и атрибутов доступа

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

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **низкая**.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения принятых правил работы с ИСПД или не осведомлены о них.

В Учреждении осуществляется резервное копирование обрабатываемых ПД, пользователи проинструктированы о работе с ИСПД.

Вероятность реализации угрозы – **маловероятна**.

Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения принятых правил работы с ИСПД и средствами защиты или не осведомлены о них.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПД.

Вероятность реализации угрозы – **маловероятна**.

Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляет резервирование ключевых элементов ИСПД.

Вероятность реализации угрозы – **маловероятна**.

Сбой системы электроснабжения

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

В Учреждении ко всем ключевым элементам ИСПД подключены источники бесперебойного питания и осуществляет резервное копирование информации.

Вероятность реализации угрозы – **маловероятна**.

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятна**.

Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПД и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Учреждении пользователи осведомлены о порядке работы с персональными данными.

Вероятность реализации угрозы – **маловероятна**.

Угрозы несанкционированного доступа по каналам связи

Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

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

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

Перехват за переделами с контролируемой зоны.

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы – **маловероятна**.

Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПД и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Вероятность реализации угрозы – **маловероятна**.

Угроза выявления паролей

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

Вероятность реализации угрозы – **маловероятна**.

Угрозы навязывание ложного маршрута сети

Данная угроза 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 хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПД. 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.

Вероятность реализации угрозы –**маловероятна.**

Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, 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 ИСПД - цели угроз.

Вероятность реализации угрозы – **маловероятна**.

Внедрение ложного объекта сети

Эта угроза 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.

Вероятность реализации угрозы – **маловероятна**.

Угрозы типа «Отказ в обслуживании»

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

Могут быть выделены несколько разновидностей таких угроз:

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

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПД при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMPRedirectHost, 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 ПД в ИСПД, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПД, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПД из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Вероятность реализации угрозы – **маловероятна.**

Угрозы удаленного запуска приложений

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

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;

- удаленный запуск приложения путем переполнения буфера приложений-серверов;

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

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

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

буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, 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.

Вероятность реализации угрозы – **маловероятна**.

Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

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

Вероятность реализации угрозы – **маловероятна**.

2. Исходный уровень защищенности ИСПД

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

В таблице представлены характеристики уровня исходной защищенности для ИСПД организации.

Таблица 1 – Исходный уровень защищенности

№ п/п	Технические и эксплуатационные характеристики	ИСПД ГИС «Электронное образование в Республике Татарстан»	ИСПД Свободное программное обеспечение «Барс-бюджет»	ИСПД Региональная информационная система ГИА	ИСПД ГИС «Электронный детский сад»
1	По территориальному размещению	0	0	0	0
2	По наличию соединения с сетями общего пользования	5	5	5	5
3	По встроенным (легальным) операциям с записями баз персональных данных	0	0	0	0
4	По разграничению доступа к персональным данным	0	0	0	0
5	По наличию соединений с	0	0	0	0

	другими базами ПД иных ИСПД				
6	По уровню (обезличивания) ПД	5	5	5	5
7	По объему ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки	0	0	0	0

3. Вероятность реализации УБПД

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

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);
- **низкая вероятность**- объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);
- **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПД недостаточны ($Y_2 = 5$);
- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПД не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПД можно выделить следующие угрозы:

4. Реализуемость 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 УБПД представлена в таблице.

Таблица 2 – Реализуемость УБПД

Тип угроз безопасности ПД	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0	низкая
1.2. Угрозы утечки видовой информации	0	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД		
2.1.1. Кража ПЭВМ	0	низкая
2.1.2. Кража носителей информации	0	низкая
2.1.3. Кража ключей и атрибутов доступа	0	низкая
2.1.4. Кражи, модификации, уничтожения информации	0	низкая

2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,3	средняя
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0	низкая
2.1.7. Несанкционированное отключение средств защиты	0	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,3	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа	0	низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,3	средняя
2.3.3. Непреднамеренное отключение средств защиты	0,3	средняя
2.3.4. Выход из строя аппаратно-программных средств	0,3	средняя
2.3.5. Сбой системы электроснабжения	0.3	средняя
2.3.6. Стихийное бедствие	0	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0	низкая
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации:	0	низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	0	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.	0	низкая
2.5.3.Угрозы выявления паролей по сети	0	низкая

2.5.4.Угрозы навязывание ложного маршрута сети	0	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях	0	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0	низкая
2.5.8.Угрозы удаленного запуска приложений	0	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0	низкая

5. Оценка опасности угроз

Оценка опасности УБПД производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПД представлена таблице.

Таблица 3 – Опасность УБПД

Тип угроз безопасности ПД	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая опасность
1.2. Угрозы утечки видовой информации	низкая опасность
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая опасность
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД	
2.1.1. Кража ПЭВМ	низкая опасность
2.1.2. Кража носителей информации	низкая опасность
2.1.3. Кража ключей и атрибутов доступа	низкая опасность
2.1.4. Кражи, модификации, уничтожения информации	низкая опасность
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	низкая опасность
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	
2.1.7. Несанкционированное отключение средств защиты	средняя опасность
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	средняя опасность
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая опасность
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	низкая опасность
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном	

обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	низкая опасность
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	средняя опасность
2.3.3. Непреднамеренное отключение средств защиты	средняя опасность
2.3.4. Выход из строя аппаратно-программных средств	средняя опасность
2.3.5. Сбой системы электроснабжения	средняя опасность
2.3.6. Стихийное бедствие	низкая опасность
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая опасность
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая опасность
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации:	низкая опасность
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая опасность
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая опасность
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая опасность
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.	низкая опасность
2.5.3.Угрозы выявления паролей по сети	низкая опасность
2.5.4.Угрозы навязывание ложного маршрута сети	низкая опасность
2.5.5.Угрозы подмены доверенного объекта в сети	низкая опасность
2.5.6.Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях	низкая опасность
2.5.7.Угрозы типа «Отказ в обслуживании»	низкая опасность
2.5.8.Угрозы удаленного запуска приложений	низкая опасность
2.5.9.Угрозы внедрения по сети вредоносных программ	низкая опасность

6. Определение актуальности угроз в ИСПД

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

Таблица 4 – Правила определения актуальности УБПД

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

Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 5 – Актуальность УБПД

Тип угроз безопасности ПД	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная
2.3.3. Непреднамеренное отключение средств защиты	актуальная
2.3.4. Выход из строя аппаратно-программных средств	актуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	неактуальная

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации:	неактуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

7. Заключение

Были выявлены следующие актуальные угрозы:

1) Действия вредоносных программ (вирусов)

Непреднамеренная модификация (уничтожение) информации сотрудниками

Непреднамеренное отключение средств защиты

Выход из строя аппаратно-программных средств

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Для снижения опасности реализации актуальных УБПД рекомендуется осуществить следующие мероприятия:

1) Провести обучение сотрудников, допущенных к обработке ПД правилам обращения с ПД, требованиям нормативных документов.

Разработать инструкции пользователей ИСПД.

Своевременно производить профилактическое обслуживание технических средств ИСПД.

При расширении и модернизации ИСПД учитывать актуальность возникновения угроз безопасности ПД.