РОССИЙСКАЯ ФЕДЕРАЦИЯ

АДМИНИСТРАЦИЯ ИЛАНСКОГО РАЙОНА

КРАСНОЯРСКОГО КРАЯ

**РАСПОРЯЖЕНИЕ**

08.05.2024 г. Иланский № 50-р

Об утверждении модели угроз безопасности информации в информационной системе Администрации Иланского района

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», руководствуясь статьями 32.3, 34 Устава:

1. Утвердить модель угроз безопасности информации (Приложение №1).

2*.* Контроль за выполнением настоящего постановления возложить на заместителя по оперативным вопросам - начальника отдела по делам гражданской обороны, чрезвычайным ситуациям и пожарной безопасности Администрации Иланского района Крутских Ю.П.

3. Распоряжениевступает в силу со дня опубликования*.*

4. Опубликовать на официальном сайте Администрации Иланского района.

Глава района О.А. Альхименко

Приложение №1

к распоряжению Администрации Иланского района

от 08.05.2024 № 50-р

МОДЕЛЬ

угроз безопасности информации в информационной системе Администрации Иланского района

1. I. Общие положения

1.1. Настоящая модель угроз содержит систематизированный перечень и описание угроз безопасности информации при их обработке в информационной системе Администрации Иланского района (далее – ИС).

1.2. Модель угроз предназначена для определения актуальных угроз и характеристик вероятного нарушителя безопасности информации, а также для определения требуемого класса криптографических средств защиты информации.

1.3. Моделирование угроз необходимо для выполнения требований законодательства Российской Федерации по защите персональных данных (Федерального закона от 27 июля 2006 года № 152-ФЗ и постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119), а также требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службой по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.4. Модель угроз разработана с учетом следующих правовых актов, нормативно-методических документов и стандартов:

- Банк данных угроз безопасности информации, размещенный на официальном сайте Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru);

- Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденная 15 февраля 2008 года приказом заместителя директора Федеральной службы по техническому и экспортному контролю России;

- Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденная 14 февраля 2008 года заместителем директора Федеральной службы по техническому и экспортному контролю России;

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 центра Федеральной службы безопасности России 21 февраля 2008 года;

- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения».

1. **II. Обозначения и сокращения**

АРМ – автоматизированное рабочее место;

ИС – информационные системы;

ИТС – информационно-телекоммуникационная сеть;

КЗ – контролируемая зона;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НДВ – недекларированные возможности;

НСД – несанкционированный доступ;

ОГВ – орган государственной власти;

ОРД – организационно-распорядительная документация;

ПАК – программно-аппаратный комплекс;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СЗИ – система защиты информации;

СрЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

СУБД – система управления базами данных;

ТКУИ – технические каналы утечки информации;

УБИ – угрозы безопасности информации.

1. III. Термины и определения

В настоящем документе используются следующие термины и их определения:

**Автоматизированная обработка -** обработка персональных данных с помощью средств вычислительной техники**.**

**Атака (сетевая атака) –** компьютерная атака с использованием протоколов межсетевого взаимодействия.

**Безопасность информации** – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

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

**Доступ в операционную среду компьютера** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы, исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

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

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

**Защита информации техническая; ТЗИ –** защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

**Защита информации криптографическая** **–** защита информации с помощью ее криптографического преобразования.

**Защита информации физическая** **–** защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

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

**Информационные ресурсы** – отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

**Информативный сигнал** – сигнал, по параметрам которого может быть определена защищаемая информация.

**Информационная система** – совокупность содержащихся в базах данных и обеспечивающих их обработку информационных технологий и технических средств.

**Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.**

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

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

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

**Модель угроз (безопасности информации)** – физическое, математическое или описательное представление свойств или характеристик угроз безопасности информации.

**Модель нарушителя** **(безопасности информации)** – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

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

**Нарушитель безопасности информации** – 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 программного обеспечения, не описанные в документации.

**Несанкционированный доступ к информации** – 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 предназначению 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.

**Оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

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

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

**Персональные данные** **биометрические** – сведения, не относящиеся к специальным категориям персональных данных, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

**Персональные данные общедоступные** – полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

**Персональные данные специальной категории** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

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

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки 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.

**Программное воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Программная закладка** – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициируют реализацию недекларированных возможностей программного обеспечения.

**Предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**Распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

**Система защиты информации** – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

**Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств приема защищаемой информации.

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

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

**Угрозы безопасности информации источник** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

**Уязвимость (информационной системы)** – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

**Фактор, воздействующий на защищаемую информацию** – явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

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

1. IV. Исходные данные для моделирования угроз

Определение угроз безопасности информации при их обработке и последующее формирование на их основе модели угроз является одним из необходимых мероприятий по обеспечению безопасности информации в информационных системах.

Выявление и учет угроз безопасности информации в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности информации при их обработке в информационных системах.

Состав и содержание угроз безопасности защищаемой информации определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации.

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы, свойств среды (пути) распространения информационных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

Угроза безопасности информации реализуется в результате образования канала реализации угрозы между источником угрозы и носителем информации, что создает необходимые условия для несанкционированного или случайного доступа к информации.

Для формирования перечня угроз и определения актуальных угроз безопасности информации в информационной системе использованы методические документы Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России и ГОСТ, приведенные в пункте 1.4.

Оценка угроз безопасности информации проведена экспертным методом по результатам информационного обследования ИС.

При моделировании угроз безопасности информации учтены:

* угрозы утечки информации по техническим каналам;
* угрозы несанкционированного доступа (НСД) к информации.
* угрозы, возникающие в результате проведения атак.

Атаки характеризуются тщательной подготовкой, выбором объектов и целей атак и средств достижения целей. Возможность проведения атак на информационные системы определяются моделью нарушителя.

* 1. **Типы объектов защиты и защищаемой информации**

В ИС подлежат защите:

информационные ресурсы (включая ПДн): базы данных, каталоги и отдельные файлы, резервные копии баз данных и файлов с защищаемой информацией – обеспечение конфиденциальности, целостности и доступности;

технологическая информация ИС: управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки СЗИ), аутентификационная информация, ключи и атрибуты доступа, информация в электронных журналах регистрации – обеспечение конфиденциальности, целостности и доступности;

системное и прикладное программное обеспечение ИС, резервные копии программного обеспечения, программное обеспечение СрЗИ – обеспечение целостности и доступности;

технические средства ИС: серверы, оборудование, предназначенное для хранения данных, коммутационное оборудование, машинные носители информации – обеспечение целостности и доступности.

* 1. **Источники угроз**

Исходя из характеристик и особенностей функционирования ИС, в качестве источников угроз ИС и защищаемой информации выступают:

1. Внутренние техногенные источники:
* сети электропитания;
* системы кондиционирования;
* технические средства обработки информации;
* программное обеспечение.
1. Антропогенные источники:
* внешние нарушители;
* внутренние нарушители.

Источниками угроз НСД могут выступать аппаратная закладка, носитель вредоносной программы или сам нарушитель.

Внедрение в ИС аппаратных закладок обусловлено деятельностью разведывательных служб иностранных государств.

Внедрение в ИС вредоносных программ возможно с использованием внешних каналов связи или отчуждаемых носителей.

Характеристики вероятного нарушителя безопасности информации определяются в модели нарушителя.

* 1. **Характеристика вероятного нарушителя**

Нарушитель реализует угрозы путем непосредственного доступа к объектам защиты (техническим и программным средствам ИС, защищаемой информации) или путем проведения атак из-за пределов контролируемой зоны, используя внешние каналы связи ИС (каналы доступа к сетям связи общего пользования и (или) международного информационного обмена).

По наличию права постоянного или разового доступа к информационной системе нарушители подразделяются на два типа: внешние и внутренние.

1) *Внешние нарушители* – нарушители, не имеющие доступа к системе, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, либо по техническим каналам утечки информации.

Возможна реализация перехвата полезного информативного сигнала ПЭМИН от технических средств ИС, создающих физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин, с помощью стационарных, портативных и автономных автоматических средств технической разведки.

Однако реализация такой угрозы безопасности информации в ИС маловероятна в связи с тем, что:

использование стационарных средств технической разведки невозможно, учитывая тактические характеристики аппаратуры разведки, ввиду отсутствия на территории Иланского района представительств (посольств, консульств) иностранных государств;

стоимость организации технической разведки не соответствует ценности добываемой информации.

ИС имеют подключения к сетям общего пользования и (или) сетям международного обмена (ИТС «Интернет»). Актуальным нарушителем для ИС могут выступать физические лица, осуществляющие атаки из-за пределов КЗ с использованием каналов доступа к ИС из внешних сетей (сетей связи общего пользования и (или) международного информационного обмена (ИТС «Интернет»)).

2) *Внутренние нарушители* – нарушители, имеющие право постоянного или разового доступа в контролируемую зону, к техническим или программным средствам ИС, включая зарегистрированных пользователей ИС, реализующие угрозы непосредственно в информационной системе.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к данным. Категории внутренних нарушителей, приведенные в базовой модели угроз Федеральной службы по техническому и экспортному контролю России, и их полномочия приведены в таблице 1.

Таблица 1 - Категории внутренних нарушителей

| Категория нарушителя | Способ доступа и полномочия |
| --- | --- |
| K1 | Лица, имеющие санкционированный доступ к ИС, но не имеющие доступа к данным (должностные лица, обеспечивающие эксплуатацию и обслуживание ИС) |
| K2 | Зарегистрированные пользователи, осуществляющие ограниченный доступ к ресурсам ИС с рабочего места |
| K3 | Зарегистрированные пользователи, осуществляющие удаленный доступ к ресурсам ИС по локальным и (или) распределенным информационным системам |
| K4 | Зарегистрированные пользователи с полномочиями администратора безопасности сегмента ИС  |
| K5 | Зарегистрированные пользователи с полномочиями системного администратора ИС  |
| K6 | Зарегистрированные пользователи с полномочиями администратора безопасности ИС  |
| K7 | Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте |
| K8 | Производители и лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИС |

Возможности внутренних нарушителей существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе по допуску сотрудников к информации и контролю порядка проведения работ.

На объектах исключено неконтролируемое пребывание посторонних лиц в пределах КЗ, либо несанкционированный доступ к техническим средствам или устройствам ввода информации ИС.

Сотрудники учреждений (нарушители категорий K1, K2, K3) имеют строго определенные права по доступу к техническим средствам (в помещения) и защищаемой информации. Все действия непривилегированных пользователей контролируются со стороны привилегированных пользователей (администраторов) с применением сертифицированных средств (в том числе СКЗИ).

Привилегированные пользователи (нарушители категорий K4, K5, K6), осуществляющие сопровождение и администрирование аппаратных и программных средств ИС и средств защиты информации, включая их настройку, конфигурирование и предоставление непривилегированным пользователям прав доступа, назначаются из числа доверенных лиц, прошедших соответствующую подготовку и обучение.

Программисты-разработчики (поставщики) прикладного ПО на объектах ИС и лица, обеспечивающие сопровождение прикладного ПО (нарушители категории K7), также относятся к категории доверенных лиц.

Все работы по поставке, сопровождению и ремонту технических средств ИС выполняются на охраняемой территории в пределах контролируемой зоны, осуществляются в присутствии доверенных лиц (администраторов). По этой причине нарушитель типа K8 также исключается из числа потенциальных внутренних нарушителей ИС.

К актуальному типу внутренних нарушителей могут быть отнесены посетители, имеющие разовое право доступа в контролируемую зону. Однако, виду принятых организационных мер, такой нарушитель не имеет бесконтрольного доступа к техническим средствам ИС и не имеет возможности осуществлять перехват (съем) информации с использованием технических средств регистрации.

Для пользователей ИС и лиц, обеспечивающих эксплуатацию, обслуживание, сопровождение и администрирование ИС, существует вероятность несанкционированных (ошибочных) действий, связанных с нарушением информационной безопасности ИС.

* + 1. **Предположения о возможностях нарушителя**

Внешний нарушитель может осуществлять перехват информации и иных данных, передаваемых по каналам связи общего пользования и (или) международного информационного обмена (Интернет), а также осуществлять компьютерные атаки на объекты защиты ИС из внешних сетей.

Внешний нарушитель имеет возможность несанкционированного доступа к каналам связи, выходящим за пределы КЗ, внедрения вредоносных программ используя подключение ИС к сетям общего пользования (ИТС «Интернет»), доступа в ИС через взаимодействующие сторонние ИС с целью добывания информации, нарушения целостности данных, навязывания ложной информации, нарушения работоспособности информационной системы, а также внедрения вредоносных программ.

Однако такой нарушитель не обладает сведениями о ключевой, парольной и аутентифицирующей информации ИС, может использовать для организации атак только доступные в свободной продаже аппаратные компоненты криптосредства и среды функционирования, средства перехвата и обработки информации в каналах связи, средства воздействия через каналы связи и общедоступные компьютерные вирусы.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ИС ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

* предотвращение и пресечение несанкционированных действий;
* подбор и расстановку кадров;
* допуск физических лиц в контролируемую зону и к средствам вычислительной техники ИС;
* контроль проведения работ на ИС.

В результате принятых мер, внутренний нарушитель не имеет возможности получения специальных знаний в объеме, необходимом для преодоления СЗИ, он лишен возможности бесконтрольного доступа к техническим средствам ИС, не имеет возможности осуществлять перехват (съем) информации с использованием технических средств регистрации. Возможность сговора внутреннего и внешнего нарушителей исключается.

* + 1. **Предположения об имеющихся у нарушителя средствах атак**

Актуальный внешний нарушитель при нахождении за пределами контролируемой зоны может использовать для несанкционированного доступа (НСД) к защищаемой информации только доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты СКЗИ. Исключается возможность применения внешним нарушителем специальных программно-технических средств реализации целенаправленных воздействий на подлежащие защите объекты.

Внутренний нарушитель для доступа к защищаемой информации может использовать только штатные программно-технические средства ИС без нарушения их целостности.

* + 1. **Описание каналов атак**

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

физический канал непосредственного доступа к объекту;

программно-аппаратные средства ИС;

электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;

кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;

незащищенные внешние каналы связи, каналы доступа к сетям общего пользования и (или) международного информационного обмена (ИТС «Интернет»).

* 1. **Аппаратная закладка**

Возможность использования аппаратной закладки для реализации НСД к защищаемой информации определяется следующими факторами:

- соответствие стоимости аппаратных закладок и сложности их скрытой установки с полученной в результате информацией;

- наличие возможности установки аппаратных закладок.

* 1. **Носитель вредоносной программы**

К наиболее опасным вредоносным программам относятся:

* компьютерные вирусы;
* программные закладки.

Возможность внедрения вредоносной программы для реализации НСД к защищаемой информации определяется следующими факторами:

* защищаемая информация представляет интерес для потенциального нарушителя;
* наличие канала внедрения вредоносных программ.

Носителем вредоносной программыможет быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

1) отчуждаемые носители: дискета, оптический диск (CD-R, CD-RW), флэш-накопитель, отчуждаемый НЖМД (HDD) и т.п.;

2) встроенные носители информации (винчестеры, процессоры, микросхемы устройств, встраиваемых в системный блок, сетевые и звуковые платы, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п.)

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

* пакеты передаваемых по компьютерной сети сообщений;
* файлы (текстовые, графические, исполняемые и т.д.).
	1. **Применение СКЗИ**

При обмене информацией между учреждениями Красноярского края посредством ИС, а также при передаче данных по кабельным системам, расположенным в пределах контролируемой зоны и не защищенных от НСД к информации организационно-техническими мерами, для обеспечения конфиденциальности информации необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу в соответствии с методическими рекомендациями Федеральной службы безопасности России.

Потенциальными нарушителями могут являться:

1. Нарушители с высоким потенциалом.
* разведывательные службы иностранных государств.
1. Нарушители со средним потенциалом.
* криминальные структуры;
* конкурирующие организации;
* недобросовестные партнеры.
1. Нарушители с низким потенциалом.
* внешние субъекты (физические лица), в том числе взломщики компьютерных систем («хакеры»);
* сотрудники Администрации Иланского района.

Доступ к защищаемой информации ИС для разведывательных служб иностранных государств и криминальных структур значительно затруднен, а конкурирующие организации и недобросовестные партнеры отсутствуют.

Комплекс мероприятий по подбору сотрудников учреждений Иланского района, а также меры контроля со стороны органов государственной безопасности и внутренних дел позволяют исключить вероятность внедрения агентов разведывательных служб иностранных государств и криминальных структур.

Зарегистрированные пользователи ИС имеют доступ к защищаемой информации в соответствии с разграничительной системой доступа и не рассматриваются в качестве актуального нарушителя, требующего применение СКЗИ.

Таким образом, для ИС актуален нарушитель с низким потенциалом, в частности взломщики компьютерных систем («хакеры»). Нарушитель данной категории действует из-за пределов контролируемой зоны путем доступа в ИС через взаимодействующие информационные системы, используя каналы связи общего пользования (ИТС «Интернет») и доступные в свободной продаже технические и программное средства.

Для нейтрализации внешнего нарушителя Н1 с базовым (низким) потенциалом требуется применение СКЗИ класса **КС1**.

При применении СКЗИ необходимо учитывать следующее:

криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ;

СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты персональных данных от раскрытия лицами, которым предоставлено право на доступ к этой информации);

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;

для обеспечения безопасности персональных данных при их обработке в ИС должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных Федеральной службой безопасности России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны Федеральной службы безопасности России (www.clsz.fsb.ru). Дополнительную информацию о конкретных средствах защиты информации рекомендуется получать непосредственно у разработчиков или производителей этих средств и, при необходимости, у специализированных организаций, проводивших тематические исследования этих средств;

в случае отсутствия прошедших в установленном порядке процедуру оценки соответствия СКЗИ, функционально пригодных для обеспечения безопасности информации при их обработке в конкретной ИС, принимается решение о разработке нового типа СКЗИ, и определяются требования к его функциональным свойствам. Решение о разработке нового типа СКЗИ может быть принято оператором в инициативном порядке в независимости от наличия СКЗИ, функционально пригодных для обеспечения безопасности персональных данных при их обработке в конкретной ИС. Разработка нового типа СКЗИ осуществляется в соответствии с Положением (ПКЗ-2005), утвержденным приказом Федеральной службы безопасности России от 9 февраля 2005 г. № 66;

СКЗИ являются как средством защиты информации, так и объектом защиты.

1. V. Моделирование угроз

Выявление и нейтрализация угроз безопасности информации в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности информации при их обработке в информационных системах ИС.

В обобщенном виде угрозы безопасности информации характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления). Подлежат оценке те угрозы безопасности информации, у которых есть источники, и источники имеют возможности и условия для реализации угроз в конкретной информационной системе.

Состав и содержание угроз безопасности информации определяется совокупностью условий и факторов, создающих опасность конфиденциальности, целостности либо доступности защищаемой информации.

Совокупность таких условий и факторов формируется с учетом характеристик информационных систем, имеющихся уязвимостей, источников угроз и имеющихся возможностей для реализации угроз. Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы.

Выявление имеющихся уязвимостей информационных систем, источников угроз, способов реализации угроз и оценка возможностей для реализации угроз составляют методологическую основу формирования модели угроз.

Перечень источников угроз информации формируются на основе опроса специалистов, персонала и должностных лиц, осуществляющих эксплуатацию и сопровождение информационных систем.

Перечень уязвимых звеньев сформирован на основании опроса IT-специалистов и сетевого сканирования IT-инфраструктуры ИС.

Перечень технических каналов утечки формируется по результатам обследования размещения технических средств ИС и технологического процесса обработки информации.

* 1. **Уязвимости ИС**
		1. **Уязвимости системного программного обеспечения**

Необходимость проведения и требования к сертификации системного программного обеспечения ИС в системе сертификации средств защиты информации по требованиям безопасности информации определяется на этапе разработки технического задания на создание ИС.

* + 1. **Уязвимости прикладного программного обеспечения**

Необходимость проведения и требования к сертификации прикладного программного обеспечения ИС в системе сертификации средств защиты информации по требованиям безопасности информации определяется на этапе разработки технического задания на создание ИС.

**5.1.3**. **Уязвимости разрабатываемого прикладного программного обеспечения**

Необходимость проведения и требования к сертификации разрабатываемого прикладного программного обеспечения ИС в системе сертификации средств защиты информации по требованиям безопасности информации определяется на этапе разработки технического задания ИС.

**5.1.4. Уязвимости продукции, предназначенной для защиты информации**

Данная группа уязвимостей нейтрализуется применением средств защиты, сертифицированных по требованиям безопасности информации.

**5.1.5. Уязвимости программной среды ИС**

Уязвимости программной среды ИС нейтрализуются применением обновлений безопасности («патчей») производителя программного обеспечения и обновлением версий программного обеспечения, устраняющих уязвимости программной среды.

**5.1.6. Уязвимости протоколов сетевого взаимодействия**

Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования, представлены в таблице 2.

Таблица 2 - Уязвимости стека протоколов TCP/IP

| Наименование протокола | Уровень стека протоколов | Наименование (характеристика) уязвимости | Содержание нарушения безопасности информации |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
| FTP (File Transfer Protocol) – протокол передачи файлов по сети | Прикладной, представи-тельный, сеансовый | 1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде).2. Доступ по умолчанию.3. Наличие двух открытых портов | возможность перехвата данных учетной  записи (имен зарегистрированных пользователей, паролей).Получение удаленного доступа к хостам |
| telnet – протокол управления удаленным терминалом  | Прикладной, представи-тельный, сеансовый | Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) | возможность перехвата данных учетной  записи пользователя.Получение удаленного доступа к хостам  |
| UDP – протокол передачи данных без установления соединения | Транспорт-ный | Отсутствие механизма предотвращения перегрузок буфера | возможность реализации UDР-шторма.В результате обмена пакетами происходит существенное снижение производительности сервера |
| ARP – протокол преобразования IP-адреса в физический адрес | Сетевой | Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде) | возможность перехвата трафика пользователя злоумышленником |
| RIP – протокол маршрутной информации | Транспорт-ный | Отсутствие аутентификации управляющих сообщений об изменении маршрута | возможность перенаправления трафика через хост злоумышленника |
| TCP – протокол управления передачей | Транспорт-ный | Отсутствие механизма проверки корректности заполнения служебных заголовков пакета | существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP |
| DNS – протокол установления соответствия имен и сетевых адресов | Прикладной, представи-тельный, сеансовый | Отсутствие средств проверки аутентификации полученных данных от источника | фальсификация ответа DNS-сервера |
| IGMP – протокол передачи сообщений о маршрутизации | Сетевой | Отсутствие аутентификации сообщений об изменении параметров маршрута | зависание систем Win 9x/NT/200 |
| SMTP – протокол сервиса доставки сообщений по электронной почте | Прикладной, представи-тельный, сеансовый | Отсутствие поддержки аутентификации заголовков сообщений | возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения |
| SNMP – протокол управления маршрутизаторами в сетях | Прикладной, представи-тельный, сеансовый | Отсутствие поддержки аутентификации заголовков сообщений | возможность переполнения пропускной способности сети |

**5.1.7. Уязвимости, вызванные наличием аппаратной закладки**

Актуальной уязвимостью можно признать возможность внедрения аппаратных закладок в серверное оборудование ИС иностранного производства следующего назначения:

- систем управления баз данных (СУБД);

- используемого для работы СЗИ.

**5.1.8. Уязвимости, обусловливающие наличие технических каналов утечки информации**

Наличие технических каналов утечки информации обусловлено функционированием технических средств ИС, сопровождающееся появлением побочных электромагнитных излучений, распространяющихся в воздушной среде, а также наводок данных излучений на технические средства, их линии и токопроводящие коммуникации, имеющие выход за пределы контролируемой зоны.

**5.1.9. Уязвимости, вызванные недостатками организации технической защиты информации**

Не на всех объектах организована строгая система доступа к техническим средствам ИС, охрана в пределах контролируемой зоны осуществляется с использованием технических средств охраны (ТСО) и систем видеонаблюдения.

* 1. **Анализ факторов, воздействующих на информацию**

На основании приведенного перечня угроз безопасности информации должны быть выявлены факторы, воздействующие на защищаемую информацию, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Факторы, воздействующие на защищаемую информацию и подлежащие анализу при обеспечении защиты информации, по признаку отношения к природе возникновения делятся на классы:

* объективные;
* субъективные.

По отношению к объекту защиты факторы, воздействующие на защищаемую информацию, подразделяются на внутренние и внешние.

Внутренние объективные факторы, воздействующие на защищаемую информацию, следующие:

* передача сигналов по проводным и оптико-волоконным линиям связи;
* излучения акустических сигналов;
* электромагнитные излучения и поля;
* ПЭМИ сигналов (видеоимпульсов) от информационных цепей и всех электрических цепей;
* модуляция ПЭМИ электромагнитными сигналами от информационных цепей, а также акустическими сигналами;
* наводки в электрических цепях ТС, цепях электропитания, заземления и линиях связи, имеющих выход за пределы помещений, в которых размещено оборудование ИС;
* акустоэлектрические преобразования в элементах ИС;
* дефекты, сбои, отказы, аварии ТС и систем ИС;
* дефекты, сбои и отказы программного обеспечения ИС.

Внешние объективные факторы, воздействующие на защищаемую информацию следующие:

* техногенного характера (сбои, отказы и аварии систем обеспечения);
* природные явления, стихийные бедствия.

Внутренние субъективные факторы, воздействующие на защищаемую информацию, следующие:

* утечка защищаемой информации, которая осуществляется за счет лиц, имеющих санкционированный доступ к ней, через:

а) передачу информации по незащищенным линиям связи;

б) обработку информации на незащищенных ТС обработки информации;

в) копирование информации на неучтенный машинный носитель информации;

г) утрату носителя информации;

* неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации путем несанкционированного копирования или изменения защищаемой информации;
* несанкционированный доступ к информации путем:

а) подключения к техническим средствам ИС;

б) использования закладочных средств (устройств);

в) использования программной среды ИС через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения ИС;

3) внесение программных закладок;

4) применение компьютерных вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) хищения носителей защищаемой информации;

д) нарушения функционирования ТС обработки информации;

* ошибки пользователей ИС при:

а) эксплуатации ТС;

б) эксплуатации программных средств;

в) эксплуатации средств и систем защиты информации;

г) вывода из эксплуатации носителей защищаемой информации.

Внешние субъективные факторы, воздействующие на защищаемую информацию, следующие:

* несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам ИС;

б) использования закладочных средств (устройств);

в) использования программной среды ИС через:

1) маскировку под зарегистрированного пользователя;

2) дефекты и уязвимости программного обеспечения;

3) внесение программных закладок;

4) применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое);

г) несанкционированного физического доступа к ИС.

* блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
* искажение, уничтожение или блокирование информации с применением программных или программно-аппаратных средств при осуществлении компьютерных или сетевых атак.
	1. **Формирование перечня угроз безопасности информации**

Основные типы угроз безопасности информации, обрабатываемой в информационных системах Администрации Иланского района, связаны с:

- перехватом (съемом) информации по техническим каналам;

- несанкционированным (в том числе случайным) доступом в ИС с использованием программных и программно-аппаратных средств.

Угрозы утечки информации по техническим каналам включают:

* угрозы утечки акустической (речевой) информации;
* угрозы утечки видовой информации;
* угрозы утечки информации по каналу ПЭМИН.

Угрозы несанкционированного доступа в ИС включают:

* угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
* угрозы, реализуемые после загрузки операционной системы с применением стандартных функций операционной системы (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.).

Имеют место угрозы НСД, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

* угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИС и принимаемой в ИС из внешних сетей информации;
* угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов, служб и соединений;
* угрозы внедрения ложного объекта в ИС;
* угрозы подмены доверенного объекта;
* угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
* угрозы выявления паролей;
* угрозы типа «Отказ в обслуживании»;
* угрозы удаленного запуска приложений;
* угрозы внедрения по сети вредоносных программ.
	1. **Характеристика угроз безопасности информации**

Описание потенциальных угроз безопасности информации включает каналы, способы реализации угроз, последствия от нарушения свойств безопасности информации конфиденциальности, целостности, доступности.

* + 1. Угрозы утечки акустической (речевой) информации

Канал утечки *акустической (речевой) информации*, содержащейся непосредственно в произносимой речи пользователя ИС, *неактуален* ввиду отсутствия в ИС голосового ввода и воспроизведения информации акустическими средствами.

* + 1. Угрозы утечки видовой информации

Канал утечки видовой информации за счет просмотра информации с экранов дисплеев и других средств отображения информации, входящих в состав ИС, неактуален ввиду принятых мер (исключена возможность неконтролируемого пребывания физических лиц в служебных помещениях, оборудование помещений, размещение средств отображения информации).

Применение специальных оптических (оптикоэлектронных) средств для добывания защищаемой информации значительно затруднено ввиду принятых в Администрации Иланского района организационно-режимных мер (жалюзи на окнах, размещение средств отображения информации, исключающее для вероятного нарушителя наличие прямого оптического канала просмотра данных, организация контролируемой зоны и пр.).

* + 1. Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации *по каналу ПЭМИН* неактуальны при условии, что СВТ удовлетворяют требованиям стандартов РФ по электромагнитной совместимости, безопасности, санитарным нормам, предъявляемым к видеодисплейным терминалам, ПЭВМ, например, ГОСТ Р 50628-93, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96.

* + 1. Использование специальных средств получения информации

Категория и ценность защищаемой информации не предполагают использование специальных средств получения информации.

Вероятность реализации угроз – маловероятна.

* + 1. Угроза внедрения аппаратных закладок

Принятые меры по организации системы доступа исключают возможность неконтролируемого пребывания физических лиц в местах размещения технических средств ИС или в непосредственной близости от них, соответственно, отсутствует возможность установки аппаратных закладок посторонними лицами. Существование данного источника угроз маловероятно также ввиду несоответствия стоимости аппаратных закладок и сложности их скрытой установки с полученной в результате информацией.

* + 1. Кража (утрата) АРМ, носителей информации

Технические средства (АРМ) и носители информации находятся в пределах контролируемой зоны (на охраняемой территории). В пределах КЗ исключено неконтролируемое пребывание посторонних лиц.

Учет носителей информации не ведется.

Вероятность реализации угрозы – средняя.

* + 1. Кража (утрата) ключей и атрибутов доступа

Ключи и атрибуты доступа в информационную систему учтены установленным порядком.

Ведется учет выдачи ключей и атрибутов доступа пользователям.

Введена персональная ответственность владельцев ключей и атрибутов доступа в информационные системы.

Вероятность реализации угрозы – низкая.

* + 1. Несанкционированные модификация, уничтожение информации

Возможно уничтожение (разглашение) информации в результате сбоев системы электроснабжения, системы защиты информации.

Возможны модификация или уничтожение информации в результате ошибочных действий пользователей.

Вероятность реализации угрозы – средняя.

* + 1. Выход из строя узлов ПЭВМ, каналов связи

Возможно уничтожение информации в результате сбоев системы электроснабжения. Возможен вывод из строя узлов ПЭВМ в результате нарушения условий эксплуатации, ошибочных действий пользователей.

Возможен вывод из строя каналов связи, расположенных за пределами контролируемой зоны в результате умышленных действий нарушителей, а также инцидентов техногенного (аварии) или природного (стихийные бедствия) характера. Вероятность реализации угрозы – средняя.

* + 1. Несанкционированное отключение (изменение настроек) средств защиты

Возможны несанкционированные отключения (изменение настроек) средств защиты в результате нарушения условий эксплуатации СЗИ или умышленных (случайных) действий пользователей или администраторов информационных систем. Вероятность реализации угрозы – высокая.

* + 1. Внедрение вредоносных программ (вирусов)

Пользователи имеют доступ к внешним сетям информационного обмена (ТКС Интернет), используют отчуждаемые (съемные) носители для информационного обмена.

Вероятность реализации угрозы – высокая.

* + 1. Недекларированные возможности системного и прикладного программного обеспечения, предназначенного для обработки информации

При применении сертифицированных средств защиты информации, обеспечивающих выполнение требований приказа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа Федеральной службы по техническому и экспортному контролю России от 18.02.13 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» происходит анализ состояния программной среды обработки персональных данных, осуществляется протоколируемый контроль действий пользователей и информационных потоков, осуществляется ограничение информационных потоков.

Вероятность реализации угрозы – маловероятна.

* + 1. Установка ПО, не связанного с исполнением служебных обязанностей

Возможны несанкционированные отключения (изменение настроек) средств защиты в результате нарушения условий эксплуатации СЗИ или умышленных (случайных) действий пользователей или администраторов информационных систем. Вероятность реализации угрозы – высокая.

* + 1. Вывод из строя технических средств, каналов связи

Возможен вывод из строя аппаратно-программных средств в результате нарушения условий эксплуатации и (или) ошибочных действий пользователей, аварий техногенного или природного характера.

Вероятность реализации угрозы – средняя.

* + 1. Сбой системы электроснабжения

Возможен вывод из строя узлов ПЭВМ, каналов связи, а также аппаратно-программных средств.

Возможно уничтожение (разглашение) информации в результате сбоев системы электроснабжения.

Вероятность реализации угрозы – низкая.

* + 1. Несанкционированный доступ (НСД) из внешних сетей

НСД к информации из внешних сетей возможен в результате реализации:

* угрозы «Анализа сетевого трафика»;
* угрозы сканирования вычислительной сети;
* угрозы внедрения ложного объекта сети;
* угрозы подмены доверенного объекта сети;
* угрозы навязывания ложного маршрута;
* угрозы выявления паролей;
* угрозы типа «Отказ в обслуживании»;
* угрозы удаленного запуска приложений;
* угрозы внедрения по сети вредоносных программ.

Вероятность реализации угроз несанкционированного доступа из внешних сетей – высокая.

5.4.17. Угрозы внедрения вредоносных программ (программно-математического воздействия)

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой 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.

Для ИС представляют опасность следующие вредоносные программы:

* классические программные (компьютерные) вирусы;
* вредоносные программы, распространяющиеся по сети (сетевые черви);
* другие вредоносные программы, предназначенные для осуществления НСД к защищаемым информационным ресурсам ИС.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в процессе разработки, сопровождения, модификации и настройки информационной системы. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Вредоносные программы основаны на использовании уязвимостей программного обеспечения различного рода, обладают широким спектром возможностей и могут действовать во всех видах программного обеспечения.

Наличие в ИС вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

Кроме того, для ИС представляют опасность:

* вывод из строя аппаратно-программных средств;
* сбой системы электроснабжения;
* кража АРМ, носителей информации;
* кража ключей и атрибутов доступа;
* вывод из строя узлов АРМ, каналов связи;
* действия вредоносных программ (вирусов);
* НДВ системного и прикладного ПО;
* несанкционированная установка ПО;
* несанкционированное отключение средств защиты.
	1. **Результаты реализации угроз безопасности информации**

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

1) *Нарушение конфиденциальности* (копирование, неправомерное распространение), которое может быть осуществлено за счет:

- копирования ее на отчуждаемые носители информации;

- несанкционированного доступа к данным из внешних сетей связи;

- восстановления информации в ходе ремонта, модификации или утилизации программно-аппаратных средств.

2)*Нарушение целостности* (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

- микропрограммы, данные и драйвера устройств ИС;

- программы и данные операционной системы;

- программы и данные прикладного программного обеспечения;

- программы и данные специального программного обеспечения;

- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;

- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;

- микропрограммы, данные и драйвера периферийных устройств вычислительной системы;

Нарушение целостности информации может быть вызвано внедрением в ИС вредоносных программ, возможно воздействие на технологическую информацию ИС, которая обеспечивает правильное функционирование информационной системы.

3) *Нарушение доступности* (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратного обеспечения или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратного обеспечения.

Указанные действия могут привести к нарушению или отказу функционирования средств обработки информации, ввода/вывода информации, хранения информации, сетевого оборудования и каналов передачи данных.

Последствия атак, связанных с реализацией протоколов межсетевого взаимодействия, приведены в таблице 3.

Таблица 3 – Характеристики сетевых атак

| №п/п | Тип атаки | Возможные последствия |
| --- | --- | --- |
| 1. | Анализ сетевого трафика | Исследование характеристик сетевого трафика, перехват передаваемых данных, идентификаторов и паролей пользователей |
| 2. | Сканирование сети | Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей |
| 3. | «Парольная» атака | Выполнение деструктивного действия, связанного с получением несанкционированного доступа |
| 4. | Подмена доверенного объекта сети | Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. |
| 5. | Навязывание ложного маршрута | Несанкционированное изменение маршрутно-адресных данных, анализ и модификация данных, навязывание ложных сообщений |
| 6. | Внедрение ложного объекта сети | Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации |
| 7. | Отказ в обслуживании | Частичное исчерпание ресурсов | Снижение пропускной способности каналов связи, производительности сетевых устройств и серверных приложений |
| Полное исчерпание ресурсов | Отсутствие доступа к среде передачи, отказ в установлении соединения, отказ в предоставлении сервиса (электронной почты, файлового и т.д.) |
| Нарушение логической связности между атрибутами, данными, объектами | Отсутствие корректных маршрутно-адресных данных, несанкционированная модификация идентификаторов, паролей |
| Использование ошибок в программах | Нарушение работоспособности сетевых устройств  |
| 8. | Удаленный запуск приложений | Путем рассылки файлов, содержащих деструктивный исполняемый код | Нарушение конфиденциальности, целостности, доступности информации |
| Путем переполнения приложения |
| Путем использования возможностей удаленного управления системой | Скрытое управление системой |

* 1. **Определение актуальных угроз безопасности информации**

На основании установленного перечня возможных угроз безопасности защищаемой информации при обработке в ИС определяются актуальные угрозы безопасности информации для ИС.

Для каждой из потенциальных угроз проводится оценка возможностей для ее реализации и степени возможного вреда. Актуальной считается угроза, которая может быть реализована и представляет опасность для информации.

Перечень актуальных угроз безопасности информации для ИС определяется в соответствии с Методикой Федеральной службы по техническому и экспортному контролю России [5].

* + 1. Определение уровня исходной защищенности ИС

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИС и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик. Результаты уточнения уровня исходной защищенности ИС приведены в таблице 4.

Таблица 4 – Уровень исходной защищенности ИС

|  |  |
| --- | --- |
| Технические и эксплуатационные характеристики ИС | Уровень защищенности |
| 1. По территориальному размещению: **распределенная ИС, охватывающая муниципальные учреждения Иланского района** | низкий |
| 2. По наличию соединения с сетями общего пользования: **имеющая многоточечный выход**  | низкий |
| 3. По встроенным (легальным) операциям с записями: **чтение, поиск, запись, удаление, сортировка, модификация, передача** | низкий  |
| 4. По разграничению доступа к данным: **имеют доступ определенные перечнем сотрудники организации** | средний |
| 5. По наличию соединений с другими базами данных: **интегрированная**  | низкий |
| 6. По уровню обобщения (обезличивания) данных: **предоставляемые данные не являются обезличенными** | низкий |
| 7. По объему данных, предоставляемых сторонним пользователям ИС: **предоставляющая часть данных** | высокий |

Уровеньисходной защищенности ИС: «*низкий»*, так как менее 70% характеристик соответствуют уровню «*средний*». Значение показателя исходной защищенности (*Y*1) равно 10.

* + 1. Определение перечня актуальных угроз

Составляем таблицу экспертной оценки угроз безопасности информации в зависимости от вероятности реализации угрозы в ИС (Таблица\_5).

Базовым показателем опасности угрозы безопасности информации в ИС является «*низкая*» опасность, т.е. реализация угрозы может привести к незначительным негативным последствиям.

Таблица 5 - Экспертная оценка угроз безопасности информации

| Тип угрозы | Показатель частоты реализации угрозы | Значение *Y***2** | Значение коэффициента реализуемости угрозы Y,*Y =(Y*1 + *Y*2)/20 | Вербальная интерпретация реализуемости угрозы | Вербальныйпоказатель опасности угрозы | Показатель актуальности угрозы |
| --- | --- | --- | --- | --- | --- | --- |
| **Угрозы от утечки по техническим каналам** |
| ***Угрозы утечки акустической информации*** | маловероятно | 0 | 0,5 | средняя | низкая | неактуальная |
| ***Угрозы утечки видовой информации*** | низкая вероятность | 2 | 0,6 | средняя | низкая | неактуальная |
| ***Угрозы утечки информации по каналам ПЭМИН*** | низкая вероятность | 2 | 0,6 | средняя | низкая | неактуальная |
| ***Использование специальных средств получения информации*** | низкая вероятность | 2 | 0,6 | средняя | низкая | неактуальная |
| **Угрозы несанкционированного доступа к информации** |
| Кража (утрата) АРМ, носителей информации | средняя вероятность | 5 | 0,75 | высокая | низкая | актуальная |
| Кража (утрата) ключей и атрибутов доступа | низкая вероятность | 2 | 0,6 | средняя | низкая | неактуальная |
| Вывод из строя узлов ПЭВМ, каналов связи | средняя вероятность | 5 | 0,75 | высокая | низкая | актуальная |
| Несанкционирован-ные модификация, уничтожение данных | средняя вероятность | 5 | 0,75 | высокая | низкая | актуальная |
| Действия вредоносных программ (вирусов) | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Несанкционированная установка ПО | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Несанкционирован-ное отключение (изменение настроек) средств защиты | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| НДВ системного и прикладного ПО  | низкая вероятность | 2 | 0,6 | средняя | низкая | неактуальная |
| Выход из строя технических средств и каналов связи | средняя вероятность | 5 | 0,75 | высокая | низкая | актуальная |
| Непреднамеренные модификация, уничтожение информации | средняя вероятность | 5 | 0,75 | высокая | низкая | актуальная |
| Анализ сетевого трафика | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Сканирование сети | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Выявления паролей | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Навязывание ложного маршрута сети | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Подмена доверенного объекта в сети | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Внедрение ложного объекта сети | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Угрозы типа «Отказ в обслуживании» | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Угрозы удаленного запуска приложений | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |
| Внедрение по сети вредоносных программ | высокая вероятность | 10 | 1 | очень высокая | низкая | актуальная |

* + 1. Перечень актуальных угроз безопасности информации

Актуальными угрозами безопасности информации в ИС признаны:

1. *Угрозы физического доступа к элементам ИС:*
* несанкционированные модификация, уничтожение информации;
* кража (утрата) АРМ, носителей информации;
* вывод из строя узлов ПЭВМ, носителей, каналов связи;
1. *Угрозы несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств:*
* внедрение вредоносных программ (вирусов);
* несанкционированная установка ПО;
* несанкционированное отключение (изменение настроек) средств защиты.
1. *Угрозы в результате непреднамеренных действий пользователей, сбоев электропитания, чрезвычайных ситуаций природного и техногенного характера (ударов молний, пожаров, наводнений и т.п.):*
* непреднамеренная модификация (уничтожение) информации;
* выход из строя технических средств и каналов связи.
1. *Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей:*
* угрозы «Анализ сетевого трафика» с перехватом передаваемой из ИС и принимаемой из внешних сетей информации;
* угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИС, топологии сети, открытых портов и служб, открытых соединений и др.;
* угрозы выявления паролей по сети;
* угрозы навязывание ложного маршрута сети;
* угрозы подмены доверенного объекта в сети;
* угрозы внедрения ложного объекта как в ИС, так и во внешних сетях;
* угрозы типа «Отказ в обслуживании»;
* угрозы удаленного запуска приложений;
* угрозы внедрения по сети вредоносных программ.
1. VI. Заключительные положения

Настоящая модель угроз безопасности информации может быть пересмотрена:

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности информации при их обработке в информационных системах муниципальных учреждений Иланского района;

Настоящий документ подлежит пересмотру и актуализации:

- в случае изменения нормативной правовой базы РФ в области информационной безопасности, требований регуляторов;

- в случае выявления дополнительных уязвимостей и угроз безопасности информации, изменения возможностей вероятного нарушителя безопасности информации.