Утверждена

распоряжением администрации муниципального района «Сосногорск»

от «\_\_30\_\_» \_\_\_\_\_12\_\_\_\_ 2016 года № 401-р

(Приложение 4)

**МОДЕЛЬ УГРОЗ**

**безопасности персональных данных**

**ИСПДн «Кадры»**

г. Сосногорск,

2016 год

**Оглавление**

[1. Обозначения и сокращения 4](#_Toc465264963)

[2. Общие положения 4](#_Toc465264964)

[3. Определение условий создания и использования персональных данных 5](#_Toc465264965)

[4. Описание форм представления персональных данных 5](#_Toc465264966)

[5. Описание информации, сопутствующей процессам создания и использования персональных данных 5](#_Toc465264967)

[6. Определение характеристик безопасности 6](#_Toc465264968)

[7. Подключение к сетям общего пользования 7](#_Toc465264969)

[8. Классификация нарушителей безопасности персональных данных 7](#_Toc465264970)

[8.1. Внешний нарушитель 8](#_Toc465264971)

[8.2. Внутренний нарушитель 8](#_Toc465264972)

[8.3. Предположения об имеющихся у нарушителя средствах реализации угроз 9](#_Toc465264973)

[9. Описание угроз безопасности 10](#_Toc465264974)

[9.1. Перечень возможных угроз безопасности 10](#_Toc465264975)

[9.1.1. Угрозы утечки акустической (речевой) информации 11](#_Toc465264976)

[9.1.2. Угрозы утечки видовой информации 11](#_Toc465264977)

[9.1.3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок 11](#_Toc465264978)

[9.1.4. Угрозы несанкционированного доступа 12](#_Toc465264979)

[9.1.5. Угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения) 12](#_Toc465264980)

[9.1.6. Угрозы, реализуемые в ходе загрузки операционной системы 13](#_Toc465264981)

[9.1.7. Угрозы, реализуемые после загрузки операционной системы 13](#_Toc465264982)

[9.1.8. Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных. 13](#_Toc465264983)

[9.1.9. Угроза «анализ сетевого трафика» с перехватом передаваемой по сети информации 14](#_Toc465264984)

[9.1.10. Угроза сканирования, направленные на выявление открытых портов и служб, открытых соединений и др. 14](#_Toc465264985)

[9.1.11. Угроза выявления паролей 14](#_Toc465264986)

[9.1.12. Угроза получения НСД путем подмены доверенного объекта 15](#_Toc465264987)

[9.1.13. Угроза навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных 15](#_Toc465264988)

[9.1.14. Угроза внедрения ложного объекта сети 15](#_Toc465264989)

[9.1.15. Угроза «Отказ в обслуживании» 15](#_Toc465264990)

[9.1.16. Угроза удаленного запуска приложений 16](#_Toc465264991)

[9.1.17. Угрозы внедрения вредоносных программ (программно-математического воздействия) 16](#_Toc465264992)

[9.1.18. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн 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 17](#_Toc465264993)

[9.2. Перечень угроз безопасности ПДн, которым подвержены конфигурационные единицы ИСПДн «Кадры» 19](#_Toc465264994)

[9.3. Оценка опасности и актуальности угроз 19](#_Toc465264995)

[9.4. Рекомендации по защите персональных данных от актуальных угроз безопасности ПДн. Описание негативных последствий воздействия вероятных нарушителей. 22](#_Toc465264996)

[Заключение 47](#_Toc465264997)

1. Обозначения и сокращения

АРМ - Автоматизированное рабочее место

ВТСС - Вспомогательные технические средства и системы

ИС - Информационная система

ИСПДн - Информационная система персональных данных

КЗ - Контролируемая зона

МЭ - межсетевой экран

НДВ - Недекларируемые возможности

НСД - Несанкционированный доступ

ОС - Операционная система

ПАО - Программно-аппаратное обеспечение

ПДн - Персональные данные

ПЗУ - Постоянно запоминающие устройства

ПО - Программное обеспечение

ППЗУ - Перепрограммируемое (перезаписываемое) запоминающее устройство

ПЭМИН - Побочное электромагнитное излучение и наводки

СВТ - Средство вычислительной техники

ТЗИ - Техническая защита информации

УБПДн - Угрозы безопасности персональных данных

ФЗ - Федеральный закон Российской Федерации

ФСБ - Федеральная служба безопасности Российской Федерации

ФСТЭК - Федеральная служба технического и экспертного контроля Российской Федерации

BIOS - BasicInput/OutputSystem — Базовая система ввода-вывода

DNS - DomainNameSystem — система доменных имен

FTP - FileTransferProtocol - протокол передачи файлов

ICMP - InternetControlMessageProtocol — протокол межсетевых управляющих сообщений

TCP - TransmissionControlProtocol - протокол управления передачей

1. Общие положения

Настоящая Модель угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) разработана во исполнение требований Федерального закона от 27.07.2006 №152 «О персональных данных», Постановления Правительства от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативно-правовых актов в области защиты персональных данных.

Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Для обеспечения безопасности ПДн при их обработке в информационных системах может осуществляться защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе, если это требуется.

При обработке персональных данных в информационной системе должно быть обеспечено: проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации; своевременное обнаружение фактов несанкционированного доступа к персональным данным; недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование; возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; постоянный контроль за обеспечением уровня защищенности персональных данных.

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

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

1. Определение условий создания и использования персональных данных

Должны быть описаны условия создания и использования персональных данных. Для этого определяются:

* субъекты, создающие персональные данные (в качестве такого субъекта может выступать лицо или его представитель в виде программного или технического средства);
* субъекты, которым персональные данные предназначены;
* правила доступа к защищаемой информации;
* информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных;
* используемые в процессе создания и использования персональных данных объекты, которые могут быть объектами угроз, создающими условия для появления угроз персональным данным. Такого рода объектами могут быть, например, технические и программные средства.

Степень детализации описания должна быть достаточной для выполнения остальных требований к этапу сбора и анализа исходных данных по информационной системе.

1. Описание форм представления персональных данных

Персональные данные имеют различные формы представления (формы фиксации) с учетом используемых в информационной системе информационных технологий и технических средств.

Необходимо дать описание этих форм представления (форм фиксации) персональных данных. К таким формам относятся области оперативной памяти, файлы, записи баз данных, почтовые отправления и т.д.

1. Описание информации, сопутствующей процессам создания и использования персональных данных

На основе анализа условий создания и использования персональных данных должна быть определена информация, сопутствующая процессам создания и использования персональных данных. При этом представляет интерес только та информация, которая может быть объектом угроз и потребует защиты.

К указанной информации, в частности, относится:

* ключевая, аутентифицирующая и парольная информация криптосредства;
* криптографически опасная информация (КОИ);
* конфигурационная информация;
* управляющая информация;
* информация в электронных журналах регистрации;
* побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражаются персональные данные или другая защищаемая информация;
* резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;
* остаточная информация на носителях информации.

В тех случаях, когда модель угроз разрабатывается лицами, не являющимися специалистами в области защиты информации, рекомендуется ограничиться приведенными выше примерами информации, сопутствующей процессам создания и использования персональных данных.

Разработчики модели угроз - специалисты в области защиты информации могут уточнить указанный выше перечень информации, сопутствующей процессам создания и использования персональных данных, с приведением соответствующих обоснований. Рекомендуется указанное уточнение делать только в случае необходимости разработки нового типа криптосредства.

Уточнение перечня информации, сопутствующей процессам создания и использования персональных данных, должно осуществляться путем:

* исключения типов рассматриваемой информации из указанного выше перечня, которые являются избыточными в силу специфики конкретной информационной системы;
* конкретизации и детализации не исключенных типов рассматриваемой информации с учетом конкретных условий эксплуатации информационной системы;
* описания типов рассматриваемой информации, не указанных в приведенном выше перечне.

1. Определение характеристик безопасности

Необходимо определить характеристики безопасности не только персональных данных, но и характеристики безопасности всех объектов, которые были определены как возможные объекты угроз.

Основными (классическими) характеристиками безопасности являются конфиденциальность, целостность и доступность.

В дополнение к перечисленным выше основным характеристикам безопасности могут рассматриваться также и другие характеристики безопасности. В частности, к таким характеристикам относятся неотказуемость[[1]](#footnote-1), учетность[[2]](#footnote-2) (иногда в качестве синонима используется термин «подконтрольность»), аутентичность*[[3]](#footnote-3)* (иногда в качестве синонима используется термин «достоверность») и адекватность[[4]](#footnote-4)*.*

Приведенный список характеристик безопасности не является исчерпывающим. Возможность большого числа характеристик безопасности кроется в определении понятия «характеристика безопасности объекта»:

«**характеристика безопасности объекта** – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства».

Как правило, условия создания и существования реальных объектов достаточно сложны и, как следствие, к ним можно предъявить достаточно много самых различных требований.

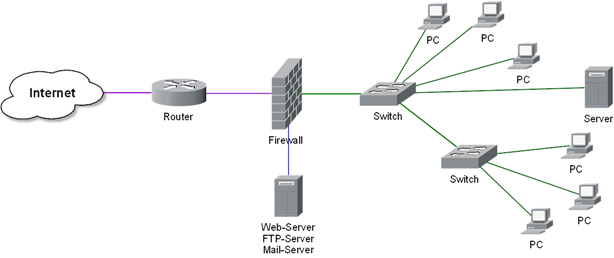
Так как угроза безопасности объекта – возможное нарушение характеристики безопасности объекта, то перечень всех характеристик безопасности для всех возможных объектов угроз, по сути, определяет модель угроз верхнего уровня.

Например, если в информационной системе требуется обеспечить только защиту от уничтожения, целостность и доступность защищаемой информации (в качестве возможного примера такой информационной системы можно привести информационную систему школьного учителя, содержащую общедоступные персональные данные учащихся), то модель угроз верхнего уровня содержит следующий перечень угроз:

* угроза уничтожения защищаемой информации;
* угроза нарушения целостности защищаемой информации;
* угроза нарушения доступности защищаемой информации.

1. Подключение к сетям общего пользования

В ИСПДн «Кадры» подключение к сетям общего пользования – **присутствует**.



1. Классификация нарушителей безопасности персональных данных

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

* внешние нарушители – физические лица, не имеющие доступа к компонентам ИСПДн «Кадры», реализующие угрозы из внешних сетей общего пользования;
* внутренние нарушители – физические лица, имеющие доступ к компонентам ИСПДн «Кадры», включая пользователей ИСПДн «Кадры», реализующих угрозы непосредственно в инфраструктуре ИСПДн «Кадры».

**Таблица 1. Категории нарушителей**

| **Тип** | **Категория ФСБ** | **Категория ФСТЭК** | **Способ и полномочия доступа** |
| --- | --- | --- | --- |
| Внешний | H1 | N0 | Не имеют санкционированного доступа к [ИСПДн «Кадры» и ПДн |
| Внутренние | H2 | N1, N8 | Имеют санкционированный доступ к ИСПДн «Кадры», но не имеют доступ к ПДн.  Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств для ИСПДн «Кадры». |
| Внутренние | H3 | N2, N3 | Зарегистрированные пользователи ИСПДн «Кадры», осуществляющие ограниченный доступ к ресурсам ИСПДн «Кадры» с рабочего места.  Зарегистрированные пользователи ИСПДн «Кадры», осуществляющие удалённый доступ к ПДн по распределённым информационным системам. |
| Внутренние | H4 | N4, N5, N6 | Зарегистрированные пользователи ИСПДн «Кадры» с полномочиями администратора безопасности сегмента безопасности ИСПДн. Зарегистрированные пользователи с полномочиями системного администратора ИСПДн «Кадры». |
| Внутренние | H5 | N7 | Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте. |
| Внутренние | H6 |  | Спецслужбы и представители специальных органов (контролирующих, правоохранительных, надзорных и т.п.) имеющих возможность применять  специальные средства и способы атак, а также специализирующиеся в области анализа СКЗИ. |

* 1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности (категория N0(Н1)) рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

К внешним нарушителям могут относиться:

а) разведывательные службы государств;

б) криминальные структуры;

в) конкуренты (конкурирующие организации);

г) недобросовестные партнеры;

д) бывшие сотрудники – администраторы или пользователи ИСПДн «Кадры»;

е) посторонние лица, пытающиеся получить доступ к информации ограниченного доступа в инициативном порядке.

Лица (категории д) хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн «Кадры» в целом, а также с применяемыми принципами и основами информационной 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).

Предполагается, что лица категории N0(Н1) относятся к вероятным нарушителям.

* 1. Внутренний нарушитель

Предполагается, что лица категории N1(Н2) и N8(Н2) могут иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн «Кадры», располагать фрагментами информации о топологии ИСПДн «Кадры» (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах, располагать именами и вести выявление паролей зарегистрированных пользователей, изменять конфигурацию технических средств ИСПДн «Кадры», вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн «Кадры».

Лица категории N2(Н3) обладают всеми возможностями лиц категории N1(Н2), знают, по меньшей мере, одно легальное имя доступа, обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн, располагают конфиденциальными данными, к которым имеют доступ. Лица категории N3(Н3) могут обладать всеми возможностями категорий N1(Н2) и N2(Н3), располагать информацией о топологии ИСПДн «Кадры» на базе распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн «Кадры», а также иметь возможность прямого (физического) доступа к фрагментам технических средств ИСПДн «Кадры».

На лиц категорий N4(Н4), N5(Н4) и N6(Н4) возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн «Кадры» для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн «Кадры». Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн «Кадры», а также к техническим и программным средствам ИСПДн «Кадры», 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 ИСПДн «Кадры» 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 для внедрения устройств негласного съема информации.

К лицам категорий N4(Н4), N5(Н4) и N6(Н4) ввиду их исключительной роли в ИСПДн «Кадры» применяется комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число лиц категорий N4(Н4), N5(Н4) и N6(Н4) включаются только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Лица категории N7(Н5) могут обладать информацией об алгоритмах и программах обработки информации на ИСПДн «Кадры», возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн «Кадры» на стадии ее разработки, внедрения и сопровождения, может располагать любыми фрагментами информации о топологии ИСПДн «Кадры» и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн «Кадры».

Нарушителей категории H6 можно исключить из числа потенциальных нарушителей, так как у данной категории есть полномочия на получение такой информации законным путем.

Таким образом, предполагается, что лица категорий N1(Н2), N2(Н3), N3(Н3), N7(Н5) и N8(Н2) относятся к вероятным нарушителям.

Сотрудники администрации муниципального района «Сосногорск» ознакомлены с Правилами обработки персональных данных в администрации муниципального района «Сосногорск» под роспись, вследствие чего предполагается, что возможность сговора внутренних нарушителей маловероятна.

* 1. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

* аппаратные компоненты ИСПДн «Кадры»;
* 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 ИСПДн «Кадры» 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 определения актуальных угроз и создания системы информационной безопасности ИСПДн «Кадры» предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, доступные в свободной продаже, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель имеет:

* средства перехвата в технических каналах утечки;
* средства воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
* средства активного воздействия на технические средства (средства облучения).

1. Описание угроз безопасности

Настоящая Модель угроз рассматривает возможность реализации всех угроз безопасности персональных данных, описанных в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК, каждым вероятным нарушителем.

* 1. Перечень возможных угроз безопасности

Выделенные выше конфигурационные единицы подвергаются (могут подвергаться) различным угрозам безопасности ПДн. Ниже приведен полный перечень возможных угроз безопасности ПДн в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

*Угрозы утечки по техническим каналам:*

* угрозы утечки акустической (речевой) информации;
* угрозы утечки видовой информации;
* угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

*Угрозы несанкционированного доступа:*

* угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения):
* угрозы, реализуемые в ходе загрузки операционной системы;
* угрозы, реализуемые после загрузки операционной системы.
* угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.:
* угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;
* угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;
* угрозы получения НСД путем подмены доверенного объекта;
* угрозы типа «Отказ в обслуживании»;
* угрозы выявления паролей;
* угрозы удаленного запуска приложений;
* угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно – адресных данных;
* угрозы внедрения ложного объекта сети.
* угрозы внедрения вредоносных программ (программно-математического воздействия):
* угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение);
* угроза внедрения по сети вредоносных программ;
* угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн 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.
  + 1. Угрозы утечки акустической (речевой) информации

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

На основе данных обследования ИСПДн «Кадры», функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют, следовательно, угрозы утечки акустической информации не подлежат рассмотрению в настоящей Модели угроз.

* + 1. Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с экранов дисплеев информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации.

Просмотр ПДн осуществляется посторонними лицами путем их непосредственного присутствия на объектах информатизации либо на расстоянии прямой видимости при отсутствии на окнах служебных кабинетов жалюзи, штор и размещения мониторов дисплеем в сторону окон из-за пределов информационных систем персональных данных с использованием оптических (оптикоэлектронных) средств (телевизионных камер, портативных аналоговых и цифровых фото- и видеокамер, встроенных в сотовые телефоны, миниатюрных видеокамер с Пинхоул-объективами).

* + 1. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанными с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации, которая используется за пределами границ контролируемой зоны.

Согласно данным обследования ИСПДн «Кадры», большинство объектов информатизации находится в непосредственной близости к сторонним организациям (размещаются в одном здании), поэтому расстояние до границы контролируемой зоны очень мало, что в свою очередь позволяет получать качественный информационный сигнал от средств обработки ПДн, размещенных в администрации муниципального района «Сосногорск» с последующей его расшифровкой. Вместе с тем, линии коммуникаций в большинстве случаев общие, что позволяет производить съем наводок от средств обработки ПДн, размещенных в администрации муниципального района «Сосногорск». Таким образом, осуществление данной угрозы возможно с территории сторонних организаций, не выдавая своего присутствия. Кроме этого перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн («аппаратурные закладки»). Предполагается, что вероятными нарушителями, осуществляющими данную угрозу, могут выступать нарушители, не имеющие прямого доступа к средствам вычислительной техники, на которых обрабатываются ПДн.

* + 1. Угрозы несанкционированного доступа

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

* угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
* угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
* угрозы внедрения вредоносных программ (программно-математического воздействия).
  + 1. Угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения)

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

* к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн с возможность перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;
* в операционную среду, то есть среду функционирования локальной операционной системы отдельного технического средства ИСПДн с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
* в среду функционирования прикладных программ (например, к локальной системе управления базами данных);
* непосредственно к информации пользователя (к файлам, текстовой, графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. Их можно объединить по условиям реализации на:

* угрозы, реализуемые в ходе загрузки операционной системы;
* угрозы, реализуемые после загрузки операционной системы.
  + 1. Угрозы, реализуемые в ходе загрузки операционной системы

Угрозы, реализуемые в ходе загрузки операционной системы, направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

* + 1. Угрозы, реализуемые после загрузки операционной системы

Угрозы, реализуемые после загрузки операционной системы, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или какой-либо прикладной программы общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

* программами просмотра и модификации реестра;
* программами поиска текстов в текстовых файлах по ключевым словам и копирования;
* специальными программами просмотра и копирования записей в базах данных;
* программами быстрого просмотра графических файлов, их редактирования или копирования;
* программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.
  + 1. Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных.

Реализация угроз создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

* содержания служебной информации в пакетах сообщений, передаваемых по сети;
* условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
* форматов представления данных (с несоответствием измененных форматов установленных для обработки по протоколам сетевого взаимодействия);
* программного обеспечения обработки данных.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств могут быть реализованы в случае удаленного доступа к ИСПДн. Их можно объединить по способам реализации на:

* угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;
* угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;
* угрозы получения НСД путем подмены доверенного объекта;
* угрозы типа «Отказ в обслуживании»;
* угрозы выявления паролей;
* угрозы удаленного запуска приложений;
* угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;
* угрозы внедрения ложного объекта сети.
  + 1. Угроза «анализ сетевого трафика» с перехватом передаваемой по сети информации

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

* изучает логику работы ИСПДн – то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий.

В дальнейшем, это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней:

* перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.
  + 1. Угроза сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.

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

* + 1. 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, установки вредоносной программы для перехвата пароля, подмены 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.

* + 1. Угроза получения НСД путем подмены доверенного объекта

Данная 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.

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

* + 1. Угроза навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных

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 ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации и управления сетью для внесения изменений в маршрутно-адресные таблицы.

* + 1. Угроза внедрения ложного объекта сети

Данная 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, 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.

* + 1. Угроза «Отказ в обслуживании»

Данная угроза основывается на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Разновидности таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping-flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к серверу;
* явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN- flooding), шторм сообщений почтовому серверу (Spam);
* явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, DNS-flooding) или идентификационной и аутентификационной информации;
* явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

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

* + 1. Угроза удаленного запуска приложений

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

* + 1. 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.

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

Программно-математическое воздействие на ИСПДн реализуется следующими угрозами:

* угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение);
* угроза внедрения по сети вредоносных программ.

Угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение) возможно осуществить только при непосредственном доступе к средствам вычислительной техники.

Описание угрозы внедрение вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение) в следующей таблице:

**Таблица 2. Описание угрозы внедрения вредоносных программ**

| **Класс вредоносной программы** | **Источник**  **угрозы** | **Способ**  **инфицирования** | **Объект**  **воздействия** | **Несанкционированный доступ** |
| --- | --- | --- | --- | --- |
| Файловые | Распространяемые по сети | Замещающие | Файлы данных, исполняемые файлы | Нарушение целостности и доступности |
| Паразитические | Исполняемые файлы |
| Компаньон-вирусы | Исполняемые файлы |
| Link-вирусы | Исполняемые файлы |
| Вирусы-черви | Исполняемые файлы |
|  |  | Вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ | Файлы данных, исполняемые файлы |  |
| Макро-вирусы | Распространяемые по сети | Использование возможностей макро-языков | Файлы данных, исполняемые файлы | Нарушение целостности |
| Загрузочные | Распространяемые по сети | Запись в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жёсткого диска | Загрузочный сектор диска и сектор, содержащий системный загрузчик жёсткого диска | Нарушение целостности и доступности |
| Сетевые | Распространяемые по сети | Использование протоколов и возможностей локальных и глобальных сетей | Файлы данных, исполняемые файлы | Нарушение целостности и доступности |

* + 1. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн 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

**Утрата ключей и атрибутов доступа**

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения инструкции парольной защиты в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их действия 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.

На основе данных обследования ИСПДн «Кадры» выявлено, что в администрации муниципального района «Сосногорск» введена парольная политика, предусматривающая приемлемую сложность пароля и периодическую его смену, пользователи ознакомлены с парольной политикой и о действиях в случаях утраты или компрометации паролей под роспись тем самым вероятность возникновения угрозы сведена к минимуму, следовательно, угроза утраты ключей и атрибутов доступа не подлежит рассмотрению в настоящей Модели угроз.

**Непреднамеренная модификация (уничтожение) информации сотрудниками**

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

На основе данных обследования ИСПДн «Кадры» выявлено, что в администрации муниципального района «Сосногорск» осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о режиме работы с ПДн под роспись тем самым вероятность возникновения угрозы сведена к минимуму, следовательно, угроза непреднамеренной модификации (уничтожения) информации сотрудниками не подлежит рассмотрению в настоящей Модели угроз.

**Непреднамеренное отключение средств защиты**

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

На основе данных обследования ИСПДн «Кадры» выявлено, что в администрации муниципального района «Сосногорск» введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе режиме работы с ПДн под роспись тем самым вероятность возникновения угрозы сведена к минимуму, следовательно, угроза непреднамеренного отключения средств защиты не подлежит рассмотрению в настоящей Модели угроз.

**Сбой системы электроснабжения**

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

На основе данных обследования ИСПДн «Кадры» выявлено, что в администрации муниципального района «Сосногорск» ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляется резервное копирование информации тем самым вероятность возникновения угрозы сведена к минимуму, следовательно, угроза сбоя системы электроснабжения не подлежит рассмотрению в настоящей Модели угроз.

**Стихийное бедствие**

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности и других внештатных ситуациях.

На основе данных обследования ИСПДн «Кадры» выявлено, что в администрации муниципального района «Сосногорск» установлена пожарная сигнализация, пользователи проинструктированы под роспись о действиях в случае возникновения внештатных ситуаций, кроме того – статистика возникновения стихийных бедствий природного характера (шторм, цунами, землетрясение и т.п.) на территории функционирования ИСПДн «Кадры» нулевая, тем самым следует предположить, что вероятность возникновения угрозы сведена к минимуму, следовательно, угроза стихийных бедствий не подлежит рассмотрению в настоящей Модели угроз.

* 1. Перечень угроз безопасности ПДн, которым подвержены конфигурационные единицы ИСПДн «Кадры»

Перечень угроз, которым подвержены конфигурационные единицы, участвующие в автоматизированной обработке ПДн в ИСПДн, входящих в состав ИСПДн «Кадры», выглядит следующим образом:

Угрозы утечки видовой информации;

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок;

Угрозы, реализуемые в ходе загрузки операционной системы;

Угрозы, реализуемые после загрузки операционной системы;

Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;

Угрозы получения НСД путем подмены доверенного объекта;

Угрозы типа «Отказ в обслуживании»;

Угрозы выявления паролей;

Угрозы удаленного запуска приложений;

Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

Угрозы внедрения ложного объекта сети;

Угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение);

Угрозы внедрения по сети вредоносных программ.

* 1. Оценка опасности и актуальности угроз

Оценка опасности угроз в ИСПДн «Кадры» произведена на основе экспертного мнения специалистов по защите информации по вербальному показателю опасности, который в соответствии с методикой определения актуальных угроз 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.

Правила, по которым УБПДн были отнесены к актуальным, соответствуют требованиям «Методики определения актуальных угроз» УФСТЭК:

**Таблица 3. Шкала актуальности угроз**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |

В случае наличия подключения к СОП

Подробно актуальность угроз безопасности ПДн представлена в следующей таблице:

**Таблица 4. Актуальность угроз**

| **№**  **п/п** | **Нарушитель** | **Вероятность реализации угрозы нарушителем категории** | **Возможность**  **реализации** | **Показатель**  **опасности**  **угрозы** | **Актуальность**  **угрозы** |
| --- | --- | --- | --- | --- | --- |
| **1** | **Угроза утечки видовой информации** | | | | |
|  | N0(Н1) | Низкая | Средняя | Высокая | Актуальна |
|  | N1(Н2) | Средняя | Высокая | Актуальна |
|  | N2(Н3) | Средняя | Высокая | Актуальна |
|  | N3(Н3) | Средняя | Высокая | Актуальна |
|  | N7(Н5) | Средняя | Высокая | Актуальна |
|  | N8(Н2) | Средняя | Высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **2** | **Угрозы утечки по каналу ПЭМИН** | | | | |
|  | N0(Н1) | Маловероятно | Средняя | Высокая | Актуальна |
|  | N1(Н2) | Маловероятно | Средняя | Актуальна |
|  | N2(Н3) | Маловероятно | Средняя | Актуальна |
|  | N3(Н3) | Маловероятно | Средняя | Актуальна |
|  | N7(Н5) | Маловероятно | Средняя | Актуальна |
|  | N8(Н2) | Маловероятно | Средняя | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **3** | **Угрозы, реализуемые в ходе загрузки ОС** | | | | |
|  | N0(Н1) | Нет прямого доступа | | | |
|  | N1(Н2) | Средняя | Высокая | Высокая | Актуальна |
|  | N2(Н3) | Средняя | Высокая | Актуальна |
|  | N3(Н3) | Средняя | Высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **4** | **Угрозы, реализуемые после загрузки ОС** | | | | |
|  | N0(Н1) | Нет прямого доступа | | | |
|  | N1(Н2) | Средняя | Высокая | Высокая | Актуальна |
|  | N2(Н3) | Средняя | Высокая | Актуальна |
|  | N3(Н3) | Средняя | Высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **5** | **Угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение)** | | | | |
|  | N0(Н1) | Нет прямого доступа | | | |
|  | N1(Н2) | Средняя | Высокая | Высокая | Актуальна |
|  | N2(Н3) | Средняя | Высокая | Актуальна |
|  | N3(Н3) | Средняя | Высокая | Актуальна |
|  | N7(Н5) | Средняя | Высокая | Актуальна |
|  | N8(Н2) | Средняя | Высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **6** | **Угроза «Анализа сетевого трафика» с перехватом передаваемой по сети информации** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **7** | **Угроза сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **8** | **Угроза получения НСД путем подмены доверенного объекта** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **9** | **Угроза типа «Отказ в обслуживании»** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **10** | **Угроза выявления паролей** | | | | |
|  | N0(Н1) | Средняя | Высокая | Высокая | Актуальна |
|  | N1(Н2) | Средняя | Высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **11** | **Угроза удаленного запуска приложений** | | | | |
|  | N0(Н1) | Средняя | Высокая | Высокая | Актуальна |
|  | N1(Н2) | Средняя | Высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **12** | **Угроза внедрения по сети вредоносных программ** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **13** | **Угроза навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |
| **14** | **Угроза внедрения ложного объекта сети** | | | | |
|  | N0(Н1) | Высокая | Очень высокая | Высокая | Актуальна |
|  | N1(Н2) | Высокая | Очень высокая | Актуальна |
|  | N2(Н3) | Высокая | Очень высокая | Актуальна |
|  | N3(Н3) | Высокая | Очень высокая | Актуальна |
|  | N7(Н5) | Высокая | Очень высокая | Актуальна |
|  | N8(Н2) | Высокая | Очень высокая | Актуальна |
|  | Итого для угрозы: |  |  |  | Актуальна |

Таким образом, перечень актуальных угроз безопасности ПДн выглядит следующим образом:

Угрозы утечки видовой информации;

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок;

Угрозы, реализуемые в ходе загрузки ОС;

Угрозы, реализуемые после загрузки ОС;

Угрозы внедрения вредоносных программ (подмена ПО на программы с НДВ, внедрение ПО с вредоносным кодом, ассоциирование штатного ПО с вредоносным ПО, вирусное заражение);

Угрозы «Анализ сетевого трафика» с перехватом передаваемой по сети информации;

Угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;

Угрозы подмены доверенного объекта;

Угрозы типа «Отказ в обслуживании»;

Угрозы удаленного запуска приложений;

Угрозы внедрения по сети вредоносных программ;

Угрозы выявления паролей;

Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

Угрозы внедрения ложного объекта сети.

* 1. Рекомендации по защите персональных данных от актуальных угроз безопасности ПДн. Описание негативных последствий воздействия вероятных нарушителей.

Актуальные угрозы безопасности ПДн, установленные в ходе изучения ИСПДн, входящих в состав ИСПДн «Кадры», представляют собой условия и факторы, создающие реальную опасность несанкционированного доступа к ПДн с целью нарушения их конфиденциальности, целостности и доступности.

В целях обоснованного подхода к обеспечению безопасности ПДн для нейтрализации актуальных угроз безопасности, выявленных согласно вышеизложенной Модели угроз, необходимо выполнить мероприятия по защите ПДн в разрезе каждой актуальной угрозы. Ниже приведены рекомендации по выполнению мероприятий по защите ПДн для каждой угрозы безопасности ПДн.

**Таблица 5. Рекомендации по защите ПДн**

| **Вид мероприятий** | **Технические меры реализации** | **Организационные меры реализации** |
| --- | --- | --- |
| Защита ПДн от утечки видовой информации | – использование хранителей экрана с вводом пароля пользователя;  – автоматическая блокировка экрана при отсутствии пользователя на рабочем месте. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр. |
| Защита ПДн от утечки информации по каналам ПЭМИН | – использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;  – экранирование аппаратных средств ИСПДн «Кадры», их соединительных линий и кабелей электропитания;  – использование сертифицированных генераторов пространственного зашумления;  – оборудование объектов информатизации, на которых ведется обработка ПДн, контурами заземления;  – развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информационный сигнал. | – размещение объектов защиты на максимально возможном расстоянии от границ КЗ;  – размещение понижающих трансформаторной подстанции электропитания и контуров заземления объектов защит в пределах контролируемой зоны;  – организация электромагнитной развязки между информационными цепями, по которым циркулирует защищаемая информация, и линиями связи, другими цепями ВТСС, выходящими за пределы КЗ;  – организация физической охраны зданий, помещений в которых размещены объекты защиты. |
| Защита ПДн от угроз, реализуемых в ходе загрузки ОС | – применение сертифицированных СЗИ от НСД;  – резервирование технических средств, дублирование массивов и носителей информации. | – организация физической охраны зданий, помещений в которых размещены объекты защиты, средств вычислительной техники, на которых ведется обработка ПДн;  – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационной системе персональных данных;  – разработка Регламента резервного копирования и восстановления персональных данных;  – разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты  информации;  – регистрация действий пользователей ИСПДн «Кадры» и обслуживающего персонала, контроль несанкционированного доступа и действия пользователей, обслуживающего персонала и посторонних лиц. |
| Защита ПДн от угроз, реализуемых после загрузки ОС | – применение сертифицированных СЗИ от НСД;  – резервирование технических средств, дублирование массивов и носителей информации. | – организация физической охраны зданий, помещений в которых размещены объекты защиты, средств вычислительной техники, на которых ведется обработка ПДн;  – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационной системе персональных данных;  – разработка Регламента резервного копирования и восстановления персональных данных;  – разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;  – регистрацию действий пользователей ИСПДн «Кадры» и обслуживающего персонала, контроль несанкционированного доступа и действия пользователей, обслуживающего персонала и посторонних лиц. |
| Защита ПДн от угроз «Анализ сетевого трафика» с перехватом передаваемой по сети информации | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – применение сертифицированных средств криптографической защиты информации.  – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз сканирования, направленные на выявление открытых портов и служб, открытых соединений и др. | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз подмены доверенного объекта | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз типа «Отказ в обслуживании» | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной систем персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Регламента резервного копирования и восстановления персональных данных;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз удаленного запуска приложений | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз выявления паролей | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  — разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз внедрения ложного объекта сети | – применение сертифицированных средств межсетевого экранирования;  – применение сертифицированных средств криптографической защиты информации. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции сотрудника органа криптографической защиты информации;  – разработка Инструкции о порядке допуска сотрудников к самостоятельной работе со средствами криптографической защиты информации;  – разработка Инструкции о порядке учета и выдачи средств криптографической защиты информации, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов;  – разработка Инструкции по обращению с сертифицированными ФСБ средствами криптографической защиты информации;  – организация допуска сотрудников для работы со средствами криптографической защиты информации только после прохождения подготовки по работе со средствами криптографической защиты информации. |
| Защита ПДн от угроз внедрения вредоносных программ (подмены ПО на программы с НДВ, внедрения ПО с вредоносным кодом, ассоциирования штатного ПО с вредоносным ПО, вирусное заражение) | – применение сертифицированных средств антивирусной защиты;  – применение сертифицированных средств защиты от НСД. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции по проведению антивирусного контроля в информационной системе персональных данных. |
| Защита ПДн от угроз внедрения по сети вредоносных программ | – применение сертифицированных средств антивирусной защиты;  – применение сертифицированных средств межсетевого экранирования. | – разработка Инструкции ответственному за организацию обработки персональных данных;  – разработка Инструкции по работе пользователей информационной системы персональных данных;  – разработка Инструкции по работе ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;  – разработка Технологической инструкции по работе администраторов безопасности информации;  – разработка Инструкции по проведению антивирусного контроля в информационной системе персональных данных. |

Описание негативных последствий воздействия вероятных нарушителей при реализации угроз безопасности несанкционированного доступа к ПДн в ИСПДн, входящих в состав ИСПДн «Кадры»:

**Таблица 5. Описание негативных последствий**

| **Источник**  **угрозы** | **Уязвимость** | **Способ**  **реализации** | **Объект**  **воздействия** | **Деструктивное**  **воздействие** |
| --- | --- | --- | --- | --- |
| **Угрозы, реализуемые в ходе загрузки операционной системы** | | | | |
| (N0)(H1) | Отсутствуют предпосылки для реализации данной угрозы т.к. отсутствует прямой доступ к средствам обработки данных | | | |
| (N1)(H2) | Уязвимость микропрограмм, прошивок ПЗУ, ППЗУ.  Уязвимости драйверов аппаратных средств.  Уязвимости операционных систем в процессе инициализации.  Уязвимости, вызванные наличием программно-аппаратной закладки.  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  - использование нештатного ПАО;  - внесение уязвимостей с использованием штатных средств: изменение конфигурации ПАО. | Информация, обрабатываемая на АРМ (узле) вычислительной сети:  - на отчуждаемых носителях информации:  - гибкие магнитные диски;  - жесткие магнитные диски;  - накопители электронной памяти типа флеш.  - на встроенных носителях долговременного хранения информации: жесткие магнитные диски;  - в средствах (портах) ввода/вывода информации:  - клавиатура;  - приводы магнитных и оптических дисков;  - порты ввода/вывода для подключения периферийных устройств. | Нарушение конфиденциальности:  - утечка информации;  - несанкционированное копирование;  - разглашение (публикация) защищаемой  информации.  Нарушение целостности (уничтожение, модификация, дезинформация):  - воздействие на микропрограммы, данные и драйвера устройств  вычислительной системы;  - воздействие на программы, данные и драйвера устройств обеспечивающие загрузку (инициализацию) ОС и СЗИ;  - воздействие на программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) ОС;  - внедрение вредоносной программы;  - внедрение программно-аппаратной закладки;  - воздействие на СЗИ.  Нарушение доступности:  - нарушение функционирования и отказы средств обработки информации;  - нарушение функционирования и отказы средств ввода/вывода информации;  - нарушение функционирования и отказы средств хранения информации. |
| (N2)(H3) |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля.  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей  программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля.  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации);  - на этапе утилизации элементов. |
| **Угрозы, реализуемые после загрузки операционной системы** | | | | |
| (N0)(H1) | Отсутствуют предпосылки для реализации данной угрозы т.к. отсутствует прямой доступ к средствам обработки данных | | | |
| (N1)(H2) | Уязвимость микропрограмм, прошивок ПЗУ, ППЗУ.  Уязвимости драйверов аппаратных  средств.  Уязвимости прикладного ПО;  Уязвимости специального ПО;  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей на  этапе эксплуатации:  - использование нештатного ПАО;  - внесение уязвимостей с использованием штатных сред-ств:  - обмен программами и данными содержащими модули (скрипты, макросы и т.д.)  - изменение конфигурации ПАО; | Информация, обрабатываемая на АРМ (узле) вычислительной сети:  - на отчуждаемых носителях информации:  - гибкие магнитные диски;  - жесткие магнитные диски;  - накопители электронной памяти типа  флеш;  - оптические компакт-диски.  - на встроенных носителях долговременного  хранения информации:  - жесткие магнитные диски;  - перепрограммируемые (перезаписываемые) запоминающие  устройства.  - в средствах обработки и хранения оперативной информации:  - оперативная память;  - кеш-памятью, буферы ввода-вывода;  - видео-память;  - оперативная память подключаемых устройств.  - в средствах (портах) ввода/вывода информации:  - клавиатура;  - манипулятор мышь;  - сканер;  - дисплей, монитор;  - принтер;  - приводы магнитных и оптических дисков;  - порты ввода/вывода для подключения  периферийных устройств. | Нарушение конфиденциальности:  - утечка информации;  - несанкционированное копирование;  - разглашение (публикация) защищаемой информации.  Нарушение целостности (уничтожение, модификация, дезинформация):  - воздействие на микропрограммы, данные и драйвера устройств вычислительной системы;  - воздействие на программы, данные и драйвера устройств обеспечивающие загрузку (инициализацию) ОС и СЗИ;  - воздействие на программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) ОС;  - внедрение вредоносной программы;  - внедрение программно-аппаратной закладки;  - воздействие на СЗИ.  Нарушение доступности:  - нарушение функ-циионирования и отказы средств обработки информации;  - нарушение функ-ционирования и отказы средств ввода/вывода информации;  - нарушение функ-ционирования и отказы средств хранения информации. |
| (N2)(H3) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  - использование нештатного ПАО;  - внесение уязвимостей с использованием штатных средств:  - обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  - изменение конфигурации ПАО;  - публикация, разглашение защищаемых сведений. |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации);  - на этапе утилизации элементов. |
| **Угроза «Анализа сетевого трафика» с перехватом передаваемой по сети информации** | | | | |
| (N0)(H1) | Уязвимости, вызванные наличием программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей протоколов сетевого взаимодействия и каналов передачи данных:  - перехват информации;  - удаленный несанкционированный доступ в систему;  - разглашение и утечка информации на незащищенные рабочие места  вычислительной сети.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации: использование нештатного ПАО. | Информация, обрабатываемая на АРМ (узле) вычислительной сети, в средствах (портах) ввода/вывода информации: информация в средствах передачи данных.  Информация в средствах реализующих сетевое взаимодействие и каналах передачи данных в сети. | Нарушение конфиденциальности:  - утечка информации;  - перехват информации в каналах передачи данных;  - разглашение (публикация) защищаемой информации. |
| (N1)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - уязвимости протоколов сетевого  взаимодействия и каналов передачи  данных:  - перехват информации;  - внедрение вредоносных программ;  - удаленный несанкционированный  доступ в систему;  - разглашение и утечка информации на  незащищенные рабочие места вычислительной сети.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  - использование нештатного ПАО;  - внесение уязвимостей с использованием  штатных средств:  - обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  - изменение конфигурации ПАО. |
| (N2)(H3) |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  - перехват информации;  - внедрение вредоносных программ;  - удаленный несанкционированный доступ в систему;  - разглашение и утечка информации на незащищенные рабочие места вычислительной сети.  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  - обход СЗИ;  - деструктивное воздействие на СЗИ;  - вскрытие или перехват пароля;  - уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  - перехват информации;  - внедрение вредоносных программ;  - удаленный несанкционированный доступ в систему;  - разглашение и утечка информации на незащищенные рабочие места вычислительной сети.  Внедрение (внесение) новых уязвимостей:  - на этапе проектирования и разработки;  - на этапе сопровождения (модернизации);  - на этапе утилизации элементов. |
| **Угроза сканирования, направленные на выявление открытых портов и служб,**  **открытых соединений и др.** | | | | |
| (N0)(H1) | Уязвимости, вызванные наличием программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей протоколов сетевого взаимодействия и  каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему. | Информация, обрабатываемая на АРМ (узле) вычислительной сети, в средствах (портах) ввода/вывода информации: информация в средствах передачи данных.  Информация в средствах реализующих сетевое взаимодействие и каналах передачи данных в  сети. | Нарушение конфиденциальности:  утечка информации: состав и конфигурация ПАО  перехват информации в каналах передачи данных: состав и конфигурация ПАО. |
| (N1)(H2) | Использование существующих уязвимостей протоколов сетевого взаимодействия и  каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на  этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием  штатных средств:  обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  изменение конфигурации ПАО. |
| (N2)(H3) | Использование существующих уязвимостей протоколов сетевого взаимодействия и  каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на  этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием  штатных средств:  обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  изменение конфигурации ПАО;  публикация, разглашение защищаемых  сведений. |
| (N3)(H3) |
| (N7)(H5) | Уязвимости прикладного ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных.  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей протоколов сетевого взаимодействия и  каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации). |
| (N8)(H2) | Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных.  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей протоколов сетевого взаимодействия и  каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза получения НСД путем подмены доверенного объекта сети** | | | | |
| (N0)(H1) | Уязвимости прикладного ПО.  Уязвимости специального ПО.  Уязвимости, вызванные наличием программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.  Уязвимости, вызванные недостатками организации ТЗИ от НСД. | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием  штатных средств: обмен программами и данными содержащими модули (скрипты, макросы и т.д.). | Информация, обрабатываемая на АРМ (узле)  вычислительной сети, в средствах (портах)  ввода/вывода информации: информация в  средствах передачи данных.  Информация в средствах реализующих сетевое  взаимодействие и каналах передачи данных в  сети. | Нарушение конфиденциальности:  утечка информации;  несанкционированное копирование;  перехват информации в каналах  передачи данных.  Нарушение целостности (уничтожение,  модификация, дезинформация):  воздействие на программы и данные  специального ПО;  внедрение вредоносной программы;  воздействие на технологическую  сетевую информацию:  средства управления сетей;  средства управления адресами и  маршрутизацией передачи данных в  сети;  средства управления  функциональным контролем сети;  средства управления безопасностью  информации в сети.  Нарушение доступности: нарушение и  отказы функционирования аппаратуры и  каналов передачи данных. |
| (N1)(H2) | Уязвимости прикладного ПО.  Уязвимости специального ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных.  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости СЗИ | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на  этапе эксплуатации: внесение уязвимостей с использованием штатных средств:  обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  изменение конфигурации ПАО. |
| (N2)(H3) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный  доступ в систему.  Внедрение (внесение) новых уязвимостей на  этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием  штатных средств:  обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  изменение конфигурации ПАО. |
| (N3)(H3) |
| (N7)(H5) | Уязвимости прикладного ПО.  Уязвимости специального ПО.  Уязвимости, вызванные наличием программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных.  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза типа «Отказ в обслуживании»** | | | | |
| (N0)(H1) | Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных.  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости программно аппаратных  средств в результате сбоев в работе,  отказов этих средств. | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перегрузка ресурсов (отказ в  обслуживании);  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему. | Информация, обрабатываемая на АРМ (узле) вычислительной сети:  на отчуждаемых носителях информации:  гибкие магнитные диски;  жесткие магнитные диски;  накопители электронной памяти типа флеш;  оптические компакт-диски.  на встроенных носителях долговременного хранения информации:  жесткие магнитные диски;  постоянные запоминающие устройства;  перепрограммируемые  (перезаписываемые) запоминающие устройства.  в средствах обработки и хранения оперативной информации:  оперативная память;  кеш-памятью, буферы ввода-вывода;  видео-память;  оперативная память подключаемых устройств.  в средствах (портах) ввода/вывода  информации:  клавиатура;  манипулятор мышь;  сканер;  дисплей, монитор;  принтер;  приводы магнитных и оптических дисков;  порты ввода/вывода для подключения периферийных устройств;  информация в средствах передачи данных.  Информация в средствах реализующих сетевое взаимодействие и каналах передачи данных в сети | Нарушение доступности:  нарушение функционирования и отказы средств обработки информации;  нарушение функционирования и отказы средств ввода/вывода информации;  нарушение функционирования и отказы  средств хранения информации;  нарушение и отказы функционирования  аппаратуры и каналов передачи  данных. |
| (N1)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перегрузка ресурсов (отказ в  обслуживании);  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием штатных средств: изменение конфигурации ПАО. |
| (N2)(H3) |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  уязвимости протоколов сетевого  взаимодействия и каналов передачи данных:  перегрузка ресурсов (отказ в  обслуживании);  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перегрузка ресурсов (отказ в  обслуживании);  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза выявления паролей** | | | | |
| (N0)(H1) | Уязвимости прикладного ПО.  Уязвимости специального ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему. | Информация, обрабатываемая на АРМ (узле)  вычислительной сети:  на встроенных носителях долговременного  хранения информации: жесткие магнитные  диски;  в средствах (портах) ввода/вывода  информации:  клавиатура;  дисплей, монитор;  информация в средствах передачи  данных.  Информация в средствах реализующих сетевое  взаимодействие и каналах передачи данных в  сети. | Нарушение конфиденциальности:  утечка информации;  несанкционированное копирование;  перехват информации в каналах  передачи данных;  разглашение (публикация) защищаемой  информации.  Нарушение целостности (уничтожение,  модификация, дезинформация):  воздействие на ПО и данные  пользователя;  воздействие на микропрограммы,  данные и драйвера устройств  вычислительной системы;  воздействие на программы и данные  (дескрипторы, описатели, структуры,  таблицы и т.д.) ОС;  воздействие на программы и данные  прикладного ПО;  воздействие на программы и данные  специального ПО;  воздействие на промежуточные  (оперативные) значения программ и  данных в процессе их обработки  средствами и устройствами  вычислительной техники;  внедрение вредоносной программы;  внедрение программно-аппаратной  закладки;  воздействие на технологическую  сетевую информацию:  средства управления сетей;  средства управления адресами и  маршрутизацией передачи данных в  сети;  средства управления  функциональным контролем сети;  средства управления безопасностью  информации в сети.  воздействие на СЗИ;  Нарушение доступности:  нарушение функционирования и отказы  средств обработки информации;  нарушение функционирования и отказы  средств ввода/вывода информации;  нарушение функционирования и отказы  средств хранения информации;  нарушение и отказы функционирования  аппаратуры и каналов передачи  данных;  нарушение и отказы функционирования  СЗИ. |
| (N1)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему;  разглашение и утечка информации на незащищенные рабочие места вычислительной сети.  использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей на этапе эксплуатации: внесение уязвимостей с использованием штатных средств путем обмена программами и данными содержащими модули (скрипты, макросы и т.д.) |
| (N2)(H3) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный  доступ в систему;  разглашение и утечка информации на незащищенные рабочие места вычислительной сети.  использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей на этапе эксплуатации: внесение уязвимостей с использованием штатных средств:  обмен программами и данными  содержащими модули (скрипты, макросы и т.д.);  публикация, разглашение защищаемых сведений. |
| (N3)(H3) |
| (N7)(H5) |  | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему;  разглашение и утечка информации на незащищенные рабочие места  вычислительной сети.  использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации). |
| (N8)(H2) |  | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему;  разглашение и утечка информации на незащищенные рабочие места вычислительной сети.  использование остаточной, неучтенной информации (сбор «мусора»).  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза удаленного запуска приложений** | | | | |
| (N0)(H1) | Уязвимости прикладного ПО.  Уязвимости специального ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных  Уязвимости, вызванные недостатками организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации: использование нештатного ПАО. | Информация, обрабатываемая на АРМ (узле)  вычислительной сети:  на отчуждаемых носителях информации;  гибкие магнитные диски;  жесткие магнитные диски;  накопители электронной памяти типа  флеш;  оптические компакт-диски.  на встроенных носителях долговременного  хранения информации:  жесткие магнитные диски;  перепрограммируемые  (перезаписываемые) запоминающие  устройства.  в средствах обработки и хранения  оперативной информации:  оперативная память;  кеш-памятью, буферы ввода-вывода  видео-память;  оперативная память подключаемых устройств.  в средствах (портах) ввода/вывода  информации:  клавиатура;  манипулятор мышь;  сканер;  дисплей, монитор;  принтер;  приводы магнитных и оптических дисков;  порты ввода/вывода для подключения  периферийных устройств;  информация в средствах передачи данных.  Информация в средствах реализующих сетевое  взаимодействие и каналах передачи данных в  сети. | Нарушение конфиденциальности:  утечка информации;  несанкционированное копирование;  перехват информации в каналах передачи данных;  разглашение (публикация) защищаемой информации.  Нарушение целостности (уничтожение, модификация, дезинформация):  воздействие на ПО и данные  пользователя;  воздействие на микропрограммы,  данные и драйвера устройств вычислительной системы;  воздействие на программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) ОС;  воздействие на программы и данные прикладного ПО;  воздействие на программы и данные  специального ПО;  воздействие на промежуточные  (оперативные) значения программ и данных в процессе их обработки средствами и устройствами  вычислительной техники;  внедрение вредоносной программы;  внедрение программно- аппаратной закладки;  воздействие на технологическую  сетевую информацию:  средства управления сетей;  средства управления адресами и  маршрутизацией передачи данных в  сети;  средства управления  функциональным контролем сети;  средства управления безопасностью информации в сети.  воздействие на СЗИ;  Нарушение доступности:  нарушение функционирования и отказы средств обработки информации;  нарушение функционирования и отказы средств ввода/вывода информации;  нарушение функционирования и отказы средств хранения информации;  нарушение и отказы функционирования аппаратуры и каналов передачи данных;  нарушение и отказы функционирования  СЗИ. |
| (N1)(H2) |  | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием штатных средств: изменение конфигурации ПАО. |
| (N2)(H3) |  |
| (N3)(H3) |  |
| (N7)(H5) |  | Использование существующих уязвимостей  программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого  взаимодействия и каналов передачи  данных:  внедрение вредоносных программ;  удаленный несанкционированный  доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения  (модернизации). |
| (N8)(H2) |  | Использование существующих уязвимостей  программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  вскрытие или перехват пароля;  уязвимости протоколов сетевого  взаимодействия и каналов передачи  данных:  внедрение вредоносных программ;  удаленный несанкционированный  доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных** | | | | |
| (N0)(H1) | Уязвимости специального ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей программно- аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи  данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием штатных средств: обмен программами и  данными содержащими модули (скрипты, макросы и т.д.) | Информация, обрабатываемая на АРМ (узле)  вычислительной сети, в средствах (портах)  ввода/вывода информации: информация в  средствах передачи данных.  Информация в средствах реализующих сетевое  взаимодействие и каналах передачи данных в сети | Нарушение конфиденциальности:  утечка информации;  несанкционированное копирование;  разглашение (публикация) защищаемой  информации.  Нарушение целостности (уничтожение,  модификация, дезинформация):  воздействие на программы и данные  (дескрипторы, описатели, структуры,  таблицы и т.д.) ОС;  воздействие на программы и данные  специального ПО;  внедрение вредоносной программы;  внедрение программно-аппаратной  закладки;  воздействие на средства управления  адресами и маршрутизацией передачи  данных в сети;  воздействие на СЗИ.  Нарушение доступности: нарушение и  отказы функционирования аппаратуры и  каналов передачи данных. |
| (N1)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием штатных средств:  обмен программами и данными содержащими модули (скрипты, макросы и т.д.);  изменение конфигурации ПАО; |
| (N2)(H3) |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  деструктивное воздействие на СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения  (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения (модернизации);  на этапе утилизации элементов. |
| **Угроза внедрения ложного объекта сети** | | | | |
| (N0)(H1) | Уязвимости специального ПО.  Уязвимости, вызванные наличием  программно-аппаратной закладки.  Уязвимости, связанные с реализацией  протоколов сетевого взаимодействия и  каналов передачи данных  Уязвимости, вызванные недостатками  организации ТЗИ от НСД.  Уязвимости СЗИ. | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный  доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации: использование нештатного ПАО. | Информация в средствах реализующих сетевое  взаимодействие и каналах передачи данных в  сети | Нарушение конфиденциальности:  утечка информации;  несанкционированное копирование;  разглашение (публикация) защищаемой  информации.  Нарушение целостности (уничтожение,  модификация, дезинформация):  воздействие на средства управления  адресами и маршрутизацией передачи  данных в сети;  воздействие на СЗИ. |
| (N1)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей на этапе эксплуатации:  использование нештатного ПАО;  внесение уязвимостей с использованием штатных средств: изменение конфигурации ПАО. |
| (N2)(H3) |
| (N3)(H3) |
| (N7)(H5) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения  (модернизации). |
| (N8)(H2) | Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО):  обход СЗИ;  уязвимости протоколов сетевого взаимодействия и каналов передачи данных:  перехват информации;  модификация данных;  внедрение вредоносных программ;  удаленный несанкционированный доступ в систему.  Внедрение (внесение) новых уязвимостей:  на этапе проектирования и разработки;  на этапе сопровождения  (модернизации);  на этапе утилизации элементов. |

Заключение

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» от 27 июля 2006 года оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. При этом блокирование (нейтрализация) актуальных угроз безопасности информации, включенных в Модель угроз, обеспечивается посредством выбора и реализации в системе защиты информации мер защиты информации. Таким образом, комплекс мероприятий по обеспечению защиты ПДн, обрабатываемых в ИСПДн, должен состоять из правовых, организационных и технических мер защиты информации.

К правовым мерам защиты относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы. Тем самым требования к обеспечению безопасности ПДн, сформированные по результатам разработки настоящей Модели угроз, должны использоваться при формировании единых требований к обеспечению безопасности информации в технологической инфраструктуре ИСПДн «Кадры» наряду с требованиями по защите иной конфиденциальной информации, а также на этапе технического проектирования единой системы информационной безопасности технологической инфраструктуры ИСПДн «Кадры».

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Технические меры защиты информации предполагают использование программных, программно-аппаратных средств защиты информации. При обработке информации с использованием средств автоматизации применение технических мер защиты является обязательным условием.

1. **Неотказуемость** – способность доказать, что действие или событие произошло таким образом, что факт действия или события не может быть опровергнут (ИСО 7498–2:99 и ИСО 13888–1:2004); [↑](#footnote-ref-1)
2. **Учетность** – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта (ИСО 7498–2:99);

   – обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту. [↑](#footnote-ref-2)
3. **Аутентичность** – свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004), идентичность объекта тому, что заявлено. [↑](#footnote-ref-3)
4. **Адекватность** – свойство соответствия преднамеренному поведению и результатам (ISO/IEC 13335–1:2004). [↑](#footnote-ref-4)