Экз. № \_\_

|  |  |
| --- | --- |
| **СОГЛАСОВАНО** | **УТВЕРЖДАЮ** |
| Руководитель направления ИБ | Представитель по доверенности |
| ООО «Программа» | ${customerName} |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г. |

**МОДЕЛЬ УГРОЗ И МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ  
${customerName}**

|  |  |
| --- | --- |
|  | **РАЗРАБОТАНО** |
|  | Аналитик по информационной безопасности |
|  | ООО «Программа» |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

г. Москва

2023 г.

**ОГЛАВЛЕНИЕ**

[1. Перечень сокращений и обозначений 3](#_Toc127198736)

[2. Термины и определения 4](#_Toc127198737)

[3. Нормативно-методическое обеспечение 7](#_Toc127198738)

[4. Общие положения 8](#_Toc127198739)

[4.1. Назначение и область действия документа 8](#_Toc127198740)

[4.2. Исходные данные для оценки угроз безопасности информации 10](#_Toc127198741)

[4.3. Наименование сторон 10](#_Toc127198742)

[5. Описание систем и сетей и их характеристика как объектов защиты 12](#_Toc127198743)

[6. Возможные негативные последствия от реализации (возникновения) угроз безопасности персональных данных 15](#_Toc127198744)

[7. Возможные объекты воздействия угроз безопасности персональных данных 17](#_Toc127198745)

[7.1. Объекты воздействия и технологии, используемые для обработки персональных данных 17](#_Toc127198746)

[7.2. Описание видов воздействия на компоненты ИСПДн, реализация которых нарушителем может привести к негативным последствиям 20](#_Toc127198747)

[8. Источники угроз безопасности информации (модель нарушителя) 22](#_Toc127198748)

[8.1. Классификация нарушителей 22](#_Toc127198749)

[8.2. Актуальные категории нарушителей 27](#_Toc127198750)

[9. Способы реализации (возникновения) угроз безопасности информации 32](#_Toc127198751)

[10. Актуальные угрозы безопасности информации 62](#_Toc127198752)

[10.1. Перечень исключаемых угроз безопасности информации 62](#_Toc127198753)

[10.2. Описание возможных сценариев реализации угроз безопасности информации 62](#_Toc127198754)

[11. Заключение 64](#_Toc127198755)

[Приложение № 1 – Схема сети ООО «111» 67](#_Toc127198756)

[Приложение № 2 – Перечень угроз безопасности персональных данных в ИСПДн ООО «111» 68](#_Toc127198757)

[Приложение № 3 – Перечень тактик и соответствующих им техник, используемых для построения сценариев реализации угроз безопасности персональных данных 221](#_Toc127198758)

[Приложение № 4 – Актуальные уязвимости ИСПДн ООО «111» 232](#_Toc127198759)

# 

# Перечень сокращений и обозначений

|  |  |
| --- | --- |
| АРМ | – автоматизированное рабочее место |
| БЦ | – бизнес-центр |
| ВПО | – вредоносное программное обеспечение |
| ЗАО | – закрытое акционерное общество |
| ЗУП | – зарплата и управление персоналом |
| ИБ | – информационная безопасность |
| ИСПДн | – информационная система персональных данных |
| ИТ | – информационные технологии |
| ООО | – общество с ограниченной ответственностью |
| ПДн | – персональные данные |
| ПО | – программное обеспечение |
| ПЭВМ | – персональный компьютер |
| РФ | – Российская Федерация |
| СЗИ | – средство защиты информации |
| УБИ | – угроза безопасности информации |
| ФЗ | – федеральный закон |
| ФСБ России | – Федеральная служба безопасности |
| ФСТЭК России | – Федеральная служба по техническому и экспортному контролю |
| ЦОД | – центр обработки данных |
| BIOS | – Basic Input-Output System |
| DNS | – Domain Name System |
| HTTP | – Hyper Text Transfer Protocol |
| OSI | – Open System Interconnection |
| TCP/IP | – Transmission Control Protocol/Internet Protocol |
| UEFI | – Unified Extensible Firmware Interface |
| URL | – Uniform Resource Locator |
| VPN | – Virtual Private Network |
| XML | – eXtensible Markup Language |

# Термины и определения

**Атака** – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.

**Безопасность информации (данных)** – состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность.

**Блокирование доступа к информации –**прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

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

**Возможности нарушителя** – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

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

**Доступность** – свойство объекта находится в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

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

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

**Канал связи** – совокупность технических устройств, обеспечивающих передачу сообщений любого вида от отправителя к получателю, осуществляемую с помощью электрических сигналов.

**Контролируемая зона** – это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность**– свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

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

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

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

**Нарушитель информационной безопасности организации;** **нарушитель информационной безопасности организации –**физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

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

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

**Носитель информации**– физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

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

**Программное обеспечение** – комплекс программ, процедур и правил, а также документации, относящихся к функционированию системы обработки данных.

**Сетевая атака** – действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

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

**Средство защиты информации** – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

**Средство защиты от несанкционированного доступа –**программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

**Средства криптографической защиты информации** – средства шифрования, средства защиты от навязывания ложной информации (имитозащиты), средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

**Субъект персональных данных** – физическое лицо, обладающее персональными данными прямо или косвенно его определяющими.

**Техническая защита информации** – деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

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

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

**Уязвимость (информационной системы); брешь** – свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации. Примечания: 1. Условием реализации угрозы безопасности, обрабатываемой в системе информации, может быть недостаток или слабое место в информационной системе. 2 Если уязвимость соответствует угрозе, то существует риск.

**Целостность информации –**способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

# Нормативно-методическое обеспечение

При разработке настоящего документа учитывались требования следующих действующих нормативных методических документах по персональным данным:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
6. Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации».
7. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
8. Общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

# Общие положения

# Назначение и область действия документа

Модель угроз и модель нарушителя ${category} ${customerName} (далее – Модель угроз) подготовлена Исполнителем – Общество с ограниченной ответственностью

Угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) ${categoryDescription}.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц ${customerName}.

Модель угроз определяет перечень угроз безопасности ПДн, актуальных для информационно-телекоммуникационной сети ${customerName}, в рамках которой развернуты ИСПДн.

Модель угроз содержит краткое описание архитектуры ИСПДн, характеристику источников угроз безопасности ПДн, в том числе модель нарушителя, и описание всех угроз безопасности ПДн, актуальных для ИСПДн.

Анализ угроз включает:

* + 1. выявление источников угрозы безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
    2. анализ возможных уязвимостей ${category} ${customerName} и их программных, программно-аппаратных средств;
    3. определение возможных способов (сценариев) реализации угроз безопасности информации;
    4. оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В документе не рассматриваются методические подходы по оценке угроз безопасности ПДн, связанных с нарушением безопасности шифровальных (криптографических) средств защиты ПДн, а также угроз, связанных с техническими каналами утечки ПДн.

Угрозы безопасности ПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности ПДн. Кроме того, Модель угроз может быть пересмотрена по решению Заказчика в следующих случаях:

* изменения требований законодательства РФ в области защиты ПДн, нормативно-правовых актов и методических документов, регулирующих защиту ПДн;
* изменения в составе основных элементов ИСПДн, которые могут повлиять на состав или актуальность угроз безопасности ПДн;
* выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности ПДн или новых сценариев реализации существующих угроз;
* включения в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

Оценка угроз безопасности ПДн включает следующие этапы:

* определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности ПДн;
* определение возможных объектов воздействия угроз безопасности ПДн;
* оценку возможности реализации (возникновения) угроз безопасности ПДн и определение их актуальности.

В основе Модели угроз лежат следующие общие принципы:

1) безопасность ПДн при ее обработке в ИСПДн обеспечивается с помощью системы защиты информации;

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

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

4) при использовании СЗИ, штатно функционирующих совместно с техническими и программными средствами, данные СЗИ способны повлиять на выполнение предъявляемых к СЗИ требований и которые образуют среду функционирования СЗИ;

5) СЗИ не может обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий;

6) нарушитель может действовать на различных этапах жизненного цикла ИСПДн или СЗИ (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств информационных систем и СЗИ).

В состав экспертной группы по оценке угроз безопасности ПДн входят:

* Руководитель направления защиты информации по законодательству ООО «Программа» – \_\_\_\_\_\_\_\_\_\_\_\_\_;
* Аналитик по информационной безопасности ООО «Программа» – \_\_\_\_\_\_\_\_\_\_\_\_\_;
* Аналитик по информационной безопасности ООО «Программа» – \_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* Сотрудник департамента службы экономической безопасности ООО «111» – \_\_\_\_\_\_\_\_\_\_\_;
* Руководитель направления развития ИТ ООО «111» – \_\_\_\_\_\_\_\_\_\_\_\_\_.

# Исходные данные для оценки угроз безопасности информации

Для разработки данной модели угроз были использованы следующие документы:

* общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России;
* отчет об обследовании порядка обработки и защиты персональных данных ООО «111».

# Наименование сторон

Обладатель информации: ${customerName}.

Заказчик/Оператор: ${customerName}.

Основной вид деятельности согласно ОКВЭД: 70.22 – Консультирование по вопросам коммерческой деятельности и управления.

Адрес местонахождения: г. \_\_\_\_\_, ул. \_\_\_\_\_, д. \_\_\_\_.

За обеспечение защиты информации в ${customerName} отвечает сотрудник департамента службы экономической безопасности ${customerName} – \_\_\_\_\_\_\_.

Исполнитель: Общество с ограниченной ответственностью «Программа».

Адрес местонахождения:

Исполнитель имеет следующие лицензии:

# ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

Перечень ИСПДн, используемых для обработки ПДн представлен в Таблице № 1.

Схема сети ${customerName} представлена в Приложении № 1.

Таблица № 1

| **№ п/п** | **Наименование ИСПДн** | **Назначение** | **Категории пользователей** | **Критичность сервиса для бизнес-процессов компании** | **Количество пользователей** | **Расположение ИСПДн** |
| --- | --- | --- | --- | --- | --- | --- |
| ${index} | ${systemName} | ${systemPurpose} | ${userCategories} | ${systemPriority} | ${userCount} | ${systemPosition} |

# ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Описание негативных последствий, наступление которых в результате реализации угроз безопасности персональных данных может привести к возникновению рисков (ущерба) представлены в Таблице № 2.

Таблица № 2

| **№ п/п** | **Виды риска (ущерба)** | **Возможные типовые негативные последствия** | **Описание последствий** |
| --- | --- | --- | --- |
| У1 | Ущерб физическому лицу | Нарушение прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах | Нарушение требований ФЗ от 26.07.2006 № 152-ФЗ «О персональных данных» |
| Финансовый, иной материальный ущерб физическому лицу | Кража ПДн работников с целью дальнейшего проведения фишинговых атак |
| Нарушение конфиденциальности (утечка) ПДн | Компенсацию убытков и морального вреда за утечку ПДн.  Потеря доверия субъектов ПДн вследствие несанкционированного распространения их ПДн |
| Разглашение ПДн |
| У2 | Ущерб юридическому лицу | Нарушение законодательства Российской Федерации | Административная, уголовная, гражданско-правовая, дисциплинарная ответственность за нарушение требований ФЗ от 26.07.2006 № 152-ФЗ «О персональных данных» |
| Необходимость дополнительных (незапланированных) затрат на выплаты компенсаций | Санкции за нарушение требований ФЗ от 26.07.2006 № 152-ФЗ «О персональных данных» |
| Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) | Выведение из строя технических средств, программного обеспечения ООО «111» |
| Необходимость дополнительных (незапланированных) затрат на восстановление деятельности | Выведение из строя технических средств, программного обеспечения ООО «111» |
| Нарушение штатного режима функционирования ИСПДн | Неспособность своевременного выполнения задач, решаемых ИСПДн ООО «111» |
| Простой ИСПДн | Неспособность своевременного выполнения задач, решаемых ИСПДн ООО «111» |
| Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) | Неспособность своевременного выполнения задач, решаемых ИСПДн ООО «111» |
| Нарушение деловой репутации | Потеря конкурентоспособности, уменьшение количества контрагентов |
| Публикация недостоверной информации на официальном сайте | Потеря доверия и уменьшение количества контрагентов |
| Использование официального сайта для распространения и управления вредоносным программным обеспечением | Распространение вредоносного ПО |
| Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени | Распространение вредоносного ПО. Потеря доверия контрагентов |

В ЭТУ ТАБЛИЦУ МЫ ВСТАВЛЯЕМ ТО ЧТО У НАС ВЫБРАЛ В ПРОГЕ НА ЭТОМ ЭТАПЕ

# Возможные объекты воздействия угроз безопасности ПЕРСОНАЛЬНЫХ ДАННЫХ

# Объекты воздействия и технологии, используемые для обработки персональных данных

Перечень технологий, применяемых в ООО «111» представлен в Таблице № 3.

Таблица № 3

|  |  |  |
| --- | --- | --- |
| №  п/п | Объекты воздействия | Применение |
| ${index} | ${objectName} | ${applies} |

Возможные объекты воздействия угроз безопасности информации при ее обработке и их компоненты:

* информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.);
* программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));
* программные средства (в том числе системное и прикладное программное обеспечение, включая серверы, системы управления базами данных);
* телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);
* средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);
* привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;
* обеспечивающие системы.

Перечень объектов воздействия представлен в Таблице № 4. Детальное описание объектов воздействия приведено в Отчете об обследовании порядка обработки и защиты персональных данных ООО «111».

Таблица № 4

| **№ п/п** | **Наименование** | **Тип серверной платформы** | **Используемое системное и прикладное ПО** | **Размещение (с привязкой к схеме топологии)** | **Функциональное назначение** | **Принадлежность к ИСПДн** |
| --- | --- | --- | --- | --- | --- | --- |
|
| 1. | HPE Gen10 | Физический | ESXi (Linux) | ЦОД1 | Сервер среды виртуализации | - |
| 2. | 1c v8-1 | Виртуальный | Windows Server 2012 R2 | ЦОД1 | Сервер приложений 1C | 1С: Управление холдингом,  1С: ЗУП, 1С: Бит-финанс |
| 3. | 1с DB1 | Виртуальный | Windows Server 2012 R2 | ЦОД1 | Сервер БД | СЭД Tessa,  ОДИН,  Корпоративный портал |
| 4. | 1c v8-2 | Виртуальный | Windows Server 2012 R2 | ЦОД1 | Сервер приложений 1C | 1С: Управление холдингом,  1С: ЗУП, 1С: Бит-финанс |
| 5. | 1c DB2 | Виртуальный | Windows Server 2016 | ЦОД1 | Сервер БД | СЭД Tessa,  Корпоративный портал |
| 6. | Exchange 2019 | Виртуальный | Windows Server 2016 | ЦОД1 | Почтовый сервер | Корпоративная почта |
| 7. | Контроллеры домена | Виртуальный | Windows Server 2012 | ЦОД1 | Контроллеры домена | Active Directory |
| 8. | Blade C7000 | Физический | Windows Server | ЦОД2 | Сервер резервного копирования | - |
| 9. | HPE DL380 G8 | Физический | ESXi (Linux) | ЦО | Сервер среды виртуализации | - |
| 10. | Сервер системы DLP | Виртуальный | Windows Server 2012 | ЦО | Сервер системы DLP | DLP система |
| 11. | HPE DL380 G7 | Физический | Windows Server 2012 | ЦО | Сервер Консультант+ | Консультант+ |
| 12. | Сервер ПО E-Staff | Виртуальный | WindowsPro 10 | ЦО | Сервер ПО E-Staff | E-Staff |

# Описание видов воздействия на компоненты ИСПДн, реализация которых нарушителем может привести к негативным последствиям

Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются:

* утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
* несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
* отказ в обслуживании компонентов (нарушение доступности);
* несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
* несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
* нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

В процессе эксплуатации систем и сетей объекты воздействия и виды воздействия на них могут дополняться и изменяться относительно их состава и видов воздействия, определенных на этапе создания данных систем и сетей. В этом случае учет изменений должен проводиться в рамках реализации мероприятий по управлению конфигурацией систем и сетей и анализу угроз безопасности информации в ходе их эксплуатации.

В Таблице № 5 представлено описание видов воздействия нарушителем на компоненты ИСПДн ООО «111». ТУТ НАДО ПОДУМАТЬ ПОКА ПУСТЬ ТАК

Таблица № 5

| **Негативные последствия** | **Объект воздействия** | **Виды воздействия** |
| --- | --- | --- |
| Ущерб физическому лицу (У1) | База данных защищаемой информации | Утечка (перехват) ПДн |
| Несанкционированный доступ к ПДн |
| Серверное оборудование | Утечка (перехват) ПДн |
| Несанкционированный доступ к серверному оборудованию |
| АРМ | Утечка (перехват) ПДн |
| Несанкционированный доступ к АРМ |
| Системное программное обеспечение | Утечка (перехват) ПДн |
| Несанкционированный доступ к системному программному обеспечению |
| Прикладное программное обеспечение | Утечка (перехват) ПДн |
| Несанкционированный доступ к прикладному программному обеспечению |
| Сетевое оборудование | Утечка (перехват) ПДн |
| Несанкционированный доступ к сетевому оборудованию |
| Сетевой трафик | Утечка (перехват) ПДн |
| Несанкционированный доступ к сетевому трафику |
| Ущерб юридическому лицу (У2) | База данных защищаемой информации | Утечка (перехват) ПДн |
| Несанкционированный доступ к ПДн |
| Несанкционированная модификация, подмена, искажение базы данных ПДн |
| Отказ доступа легитимных пользователей к базе данных ПДн |
| Серверное оборудование | Утечка (перехват) ПДн |
| Несанкционированный доступ к серверному оборудованию |
| Несанкционированная модификация (подмена) компонентов серверного оборудования |
| Отказ в обслуживании серверного оборудования |
| Нарушение функционирования (работоспособности) серверного оборудования |
| Несанкционированное использование вычислительных ресурсов серверного оборудования в интересах решения несвойственных ему задач |
| АРМ | Утечка (перехват) ПДн |
| Несанкционированный доступ к АРМ |
| Несанкционированная модификация, подмена компонентов АРМ |
| Отказ в обслуживании АРМ |
| Нарушение функционирования (работоспособности) АРМ |
| Системное программное обеспечение | Утечка (перехват) ПДн |
| Несанкционированный доступ к системному программному обеспечению |
| Несанкционированная модификация, подмена, искажение системного программного обеспечения |
| Отказ в обслуживании системного программного обеспечения |
| Нарушение функционирования (работоспособности) системного программного обеспечения |
| Прикладное программное обеспечение | Утечка (перехват) ПДн |
| Несанкционированный доступ к прикладному программному обеспечению |
| Несанкционированная модификация, подмена, искажение прикладного программного обеспечения |
| Отказ в обслуживании прикладного программного обеспечения |
| Нарушение функционирования (работоспособности) прикладного программного обеспечения |
| Сетевое оборудование | Утечка (перехват) ПДн |
| Несанкционированный доступ к сетевому оборудованию |
| Несанкционированная модификация, подмена системного сетевого оборудования |
| Отказ в обслуживании сетевого оборудования |
| Нарушение функционирования (работоспособности) сетевого оборудования |
| Сетевой трафик | Утечка (перехват) ПДн |
| Несанкционированный доступ к сетевому трафику |
| Несанкционированная модификация, подмена, искажение сетевого трафика |

# ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (МОДЕЛЬ НАРУШИТЕЛЯ)

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

# Классификация нарушителей

Под нарушителем безопасности информации (далее – Нарушитель) понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение характеристик безопасности защищаемых информационных ресурсов.

Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам информационной системы, а также анализа возможностей нарушителей по доступу к компонентам информационной системы исходя из структурно-функциональных характеристик и особенностей функционирования информационной системы.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

1. *внешние нарушители (тип I)* – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
2. *внутренние нарушители (тип II)* – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Лица, имеющие право доступа в контролируемую зону, также могут осуществлять атаки из-за пределов контролируемой зоны. В таком случае, данные нарушители рассматриваются как внешние.

По признаку доступа в контролируемую зону все возможные нарушители также делятся на 2 категории:

1. категория I – лица, не имеющие права доступа в контролируемую зону;
2. категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону.

Виды нарушителей, характерных для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования, определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации угроз безопасности информации этими нарушителями.

Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

* базовыми возможностями по реализации угроз безопасности информации (Н1);
* базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
* средними возможностями по реализации угроз безопасности информации (Н3);
* высокими возможностями по реализации угроз безопасности информации (Н4).

Для одной системы или сети актуальными могут являться нарушители, имеющие разные уровни возможностей.

Для наиболее точного классифицирования нарушителей безопасности информации принято использование, с учетом основных положений Методики оценки угроз безопасности информации.

Оценка возможностей нарушителей проводится при условии, что для повышения своих возможностей нарушители могут вступать в сговор с другими видами нарушителей. При этом цели (мотивация) и возможности нарушителей подлежат объединению.

Возможные цели реализации угроз безопасности информации нарушителями представлены в Таблице № 6.

Таблица № 6

| **№ п/п** | **Вид нарушителя** | **Типы нарушителя** | **Возможные цели (мотивация)** |
| --- | --- | --- | --- |
| 1 | Отдельные физические лица (хакеры) | внешний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса) |
| 2 | Конкурирующие организации | внешний | Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды |
| 3 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
| 4 | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
| 5 | Авторизованные пользователи систем и сетей | внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| 6 | Бывшие работники (пользователи) | внешний | Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия |
| 7 | Системные администраторы информационной системы и администраторы безопасности | внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия |
| 8 | Преступные группы (криминальные структуры) | внешний | Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса) |
| 9 | Разработчики, производители, поставщики программных, технических и программно-технических средств | внутренний | Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
| 10 | Специальные службы иностранных государств (блоков государств) | внешний | Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса |
| 11 | Террористические, экстремистские группировки | внешний | Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций |
| 12 | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | внешний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |
| 13 | Поставщики вычислительных услуг, услуг связи | внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ |

Уровни возможностей нарушителей по реализации угроз безопасности информации представлены в Таблице № 7.

Таблица № 7

| **№** | **Уровень возможностей нарушителей** | **Возможности нарушителей по реализации угроз безопасности информации** | **Виды нарушителей** |
| --- | --- | --- | --- |
| Н1 | Нарушитель, обладающий базовыми возможностями | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним.  Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов | Физическое лицо (хакер);  Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;  Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.);  Авторизованные пользователи систем и сетей;  Бывшие работники (пользователи) |
| Н2 | Нарушитель, обладающий  базовыми повышенными возможностями | Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.  Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей | Преступные группы (два лица и более, действующие по единому плану);  Конкурирующие организации;  Поставщики вычислительных услуг, услуг связи;  Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;  Системные администраторы и администраторы безопасности |
| Н3 | Нарушитель, обладающий средними возможностями | Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей | Террористические, экстремистские группировки;  Разработчики, производители, поставщики программных, технических и программно-технических средств |
| Н4 | Нарушитель, обладающий высокими возможностями | Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей.  Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей | Специальные службы иностранных государств |

# Актуальные категории нарушителей

Наибольшими возможностями для нанесения ущерба организации обладают ее собственные работники. В этом случае содержанием деятельности нарушителя является прямое нецелевое использование предоставленных прав физического и (или) логического доступа. При этом он будет стремиться к сокрытию следов своей деятельности.

Лица, обладающие полномочиями системного администратора или администратора безопасности, осуществляют управление правами доступа к объектам автоматизированной системы. Эти сотрудники потенциально могут реализовывать угрозы безопасности информации, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, в соответствии с установленными для них административными полномочиями.

Основания исключения нарушителей безопасности информации из рассмотрения в Модели угроз:

1. специальные службы иностранных государств не обладают достаточной мотивацией в нарушении свойств безопасности защищаемой информации в ООО «111», т.к. защищаемая информация не затрагивает интересов других государств;
2. разработчики, производители, поставщики программных, технических и программно-технических средств дорожат своей репутацией и не заинтересованы в возникновении уязвимостей в системе;
3. лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем дорожат своей репутацией и не заинтересованы в возникновении уязвимостей в системе;
4. поставщики вычислительных услуг, услуг связи дорожат своей репутацией и не заинтересованы в возникновении уязвимостей в системе.

Модель нарушителя исключает возможность сговора доверенных лиц с нарушителями. Сговор нарушителей образует нового нарушителя. В случае сговора, категория и группа нового нарушителя будет определена максимальным показателем каждого из нарушителей, участвующих в сговоре.

Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации представлены в Таблице № 8.

Результат определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности представлен в Таблице № 9.

НАМ ПРОЩЕ ВСЕГО ТЕКСТОМ НАПИСАТЬ АКТУАЛЬНЫХ НАРУШИТЕЛЕЙ КОТОРЫХ МЫ ВЫБРАЛИ БЕЗ ТАБЛИЦЫ КОТРОАЯ НИЖЕ

Таблица № 8

|  |  |  |  |
| --- | --- | --- | --- |
| **Виды нарушителей** | **Возможные цели реализации угроз безопасности информации** | | **Соответствие целей видам риска (ущерба) и возможным негативным последствиям** |
| **Нанесение ущерба физическому лицу** | **Нанесение ущерба юридическому лицу** |
| Отдельные физические лица (хакеры) | + | + | У1:  Нарушение прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах  Финансовый, иной материальный ущерб физическому лицу  Нарушение конфиденциальности (утечка) ПДн  Разглашение ПДн  У2:  Нарушение законодательства Российской Федерации  Необходимость дополнительных (незапланированных) затрат на выплаты компенсаций  Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)  Необходимость дополнительных (незапланированных) затрат на восстановление деятельности  Нарушение штатного режима функционирования ИСПДн  Простой ИСПДн  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)  Нарушение деловой репутации  Публикация недостоверной информации на официальном сайте  Использование официального сайта для распространения и управления вредоносным программным обеспечением  Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени |
| Конкурирующие организации | + | + |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | + | + |
| Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | + | + |
| Авторизованные пользователи систем и сетей | + | + |
| Бывшие работники (пользователи) | + | + |
| Системные администраторы информационной системы и администраторы безопасности | + | + |
| Преступныегруппы (криминальные структуры) | + | + |

|  |  |  |  |
| --- | --- | --- | --- |
| **Виды нарушителей** | **Возможные цели реализации угроз безопасности информации** | | **Соответствие целей видам риска (ущерба) и возможным негативным последствиям** |
| **Нанесение ущерба физическому лицу** | **Нанесение ущерба юридическому лицу** |
| Террористические, экстремистские группировки | – | + | У2:  Нарушение законодательства Российской Федерации  Необходимость дополнительных (незапланированных) затрат на выплаты компенсаций  Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)  Необходимость дополнительных (незапланированных) затрат на восстановление деятельности  Нарушение штатного режима функционирования ИСПДн  Простой ИСПДн  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)  Нарушение деловой репутации  Публикация недостоверной информации на официальном сайте  Использование официального сайта для распространения и управления вредоносным программным обеспечением  Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени |

Таблица № 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Виды риска (ущерба) и возможные негативные последствия** | **Виды актуального нарушителя** | **Категория нарушителя** | **Уровень возможностей нарушителя** |
| 1. | У1: Нарушение прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) ПДн. Разглашение ПДн | Отдельные физические лица (хакеры) | внешний | Н1 |
| Конкурирующие организации | внешний | Н2 |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | внутренний | Н2 |
| Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | внутренний | Н1 |
| Авторизованные пользователи систем и сетей | внутренний | Н1 |
| Бывшие работники (пользователи) | внешний | Н1 |
| Системные администраторы информационной системы и администраторы безопасности | внутренний | Н2 |
| Преступныегруппы (криминальные структуры) | внешний | Н2 |
| 2. | У2: Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение штатного режима функционирования ИСПДн. Простой ИСПДн. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Нарушение деловой репутации. Публикация недостоверной информации на официальном сайте. Использование официального сайта для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. | Отдельные физические лица (хакеры) | внешний | Н1 |
| Конкурирующие организации | внешний | Н2 |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | внутренний | Н2 |
| Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | внутренний | Н1 |
| Авторизованные пользователи систем и сетей | внутренний | Н1 |
| Бывшие работники (пользователи) | внешний | Н1 |
| Системные администраторы информационной системы и администраторы безопасности | внутренний | Н2 |
| Преступныегруппы (криминальные структуры) | внешний | Н2 |
| Террористические, экстремистские группировки | внешний | Н3 |

# Способы реализации (возникновения) угроз безопасности информации

Основными способами реализации (возникновения) угроз безопасности информации являются:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) нарушение безопасности при оказании услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

7) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в соответствии с Методикой. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности информации и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

* внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
* интерфейсы для пользователей;
* интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
* возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определяются на аппаратном, системном и прикладном уровнях систем и сетей, а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

По результатам оценки возможных способов реализации угроз безопасности информации определяются:

а) виды и категории нарушителей, которые имеют возможность использования актуальных способов;

б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

В Таблице № 10 представлены актуальные способы реализации угроз безопасности информации.

Таблица № 10

| **№ п/п** | **Вид**  **нарушителя** | **Объекты воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| --- | --- | --- | --- | --- |
|  | Отдельные физические лица (хакеры)  Внешний  (Н1) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Серверное оборудование | Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
|  | Бывшие работники (пользователи)  Внешний  (Н1) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Серверное оборудование | Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
|  | Преступные группы (криминальные структуры)  Внешний  (Н2) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Серверное оборудование | Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
|  | Конкурирующие организации  Внешний  (Н2) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Серверное оборудование | Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
|  | Террористические, экстремистские группировки  Внешний  (Н3) | База данных | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
| Серверное оборудование | Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Формирование и использование скрытых каналов для передачи конфиденциальных данных |
|  | Авторизованные пользователи систем и сетей  Внутренний  (Н1) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
|  | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)  Внутренний  (Н1) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Серверное оборудование | Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
|  | Системные администраторы информационной системы и администраторы безопасности  Внутренний  (Н2) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Серверное оборудование | Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
|  | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ  Внутренний  (Н2) | База данных защищаемой информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Серверное оборудование | Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| АРМ | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Системное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Прикладное ПО | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевое оборудование | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др. | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Интерфейсы для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам |
| Ошибочные действия в ходе создания и эксплуатации систем и сетей |
| Сетевой трафик | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными системами или сетями | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |
| Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей ПО, уязвимостей архитектуры и конфигурации систем и сетей |
| Внедрение ВПО |
| Использование недекларированных возможностей ПО и (или) программно-аппаратных средств |

# Актуальные угрозы безопасности информации

# Перечень исключаемых угроз безопасности информации

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), заполнение которого осуществляется ФСТЭК России. Перечень и описание угроз актуальных для ИСПДн ООО «111» представлены в Приложении № 2.

В данной Модели угроз не рассматриваются внешние нарушители, обладающие высокими возможностями, и внутренние нарушители, обладающие средними и высокими возможностями, следовательно, угрозы – УБИ.5, УБИ.24, УБИ.35, УБИ.92, УБИ.137, УБИ.194, УБИ.195, УБИ.196, УБИ.210, УБИ.213, являются неактуальными.

С учетом структурно-функциональных характеристик ИСПДн ООО «111», не являются актуальными угрозы, связанные с применением следующих технологий:

– управление грид-системами (УБИ.1, УБИ.2, УБИ.47, УБИ.81, УБИ.110, УБИ.147);

– использование технологии суперкомпьютера (УБИ.29, УБИ.82, УБИ.106, УБИ.146, УБИ.161);

– использование технологий хранилища больших данных (УБИ.38, УБИ.50, УБИ.57, УБИ.60, УБИ.97, УБИ.105, УБИ.136, УБИ.148);

– использование оборудования с ЧПУ (УБИ.112, УБИ.204, УБИ.206, УБИ.207);

– использование Smart-карт (УБИ.216);

– использование многофакторной аутентификации (УБИ.181);

– использование съемных носителей информации (УБИ.71, УБИ.156, УБИ.158);

– использование технологий машинного обучения (УБИ.218, УБИ.219, УБИ.222);

– использование технологий искусственного интеллекта (УБИ.220, УБИ.221);

– использование технологий трансграничной передачи (УБИ.40);

– использование автоматизированной системы управления технологическим процессом (УБИ.94, УБИ.176, УБИ.177, УБИ.183).

# Описание возможных сценариев реализации угроз безопасности информации

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с Методикой **Ошибка! Источник ссылки не найден.**, и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик (тактических задач) и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, приведен в Приложении № 3.

# Заключение

В Приложении № 2 представлены актуальные угрозы безопасности персональных данных в ИСПДн ООО «111», в соответствии с банком данных угроз ФСТЭК России.

Согласно Банку угроз ФСТЭК России, были выявлены следующие актуальные угрозы безопасности персональных данных в ИСПДн ООО «111», представленные в Таблице № 11.

Таблица № 11

| **№ п/п** | **Идентификатор УБИ** | **Название** | **Возможность реализации угрозы** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

В Приложении № 4 представлены актуальные уязвимости для ИСПДн ООО «111», в соответствии с банком угроз ФСТЭК России.

Согласно Банку угроз ФСТЭК России, были выявлены следующие актуальные уязвимости для ИСПДн ООО «111»:

* .

ПРИЛОЖЕНИЕ № 1 – Схема сети ООО «111»

ПРИЛОЖЕНИЕ № 2 – Перечень угроз безопасности персональных данных в ИСПДн ООО «111»

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ УБИ** | **Наименование УБИ** | **Негативные последствия реализации угрозы** | **Объект воздействия угрозы** | **Вид нарушителя** | **Способы реализации угрозы** | **Сценарий реализации** | **Применимость угрозы для ИС** | **Актуальность угрозы** |
| 3 | Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации | У1: Нарушение прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) ПДн. Разглашение ПДн  У2: Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Нарушение штатного режима функционирования ИСПДн. Простой ИСПДн. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Нарушение деловой репутации. Публикация недостоверной информации на официальном сайте. Использование официального сайта для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. | Метаданные, системное ПО | Внутренний и внешний нарушитель с базовыми повышенными и средними возможностями | | | Применима | Да |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Использование уязвимостей ПО, архитектуры и конфигурации систем и сетей. Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам. Ошибочные действия в ходе создания и эксплуатации систем и сетей | Т1.3, Т1.5, Т1.6, Т1.11, Т1.12, Т1.13, Т1.14, Т1.16, Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.15 |
| Системные администраторы информационной системы и администраторы безопасности | Использование уязвимостей ПО, архитектуры и конфигурации систем и сетей. Ошибочные действия в ходе создания и эксплуатации систем и сетей | Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.15 |
| Конкурирующие организации | Использование уязвимостей ПО, архитектуры и конфигурации систем и сетей | Т1.3, Т1.5, Т1.6, Т1.11, Т1.12, Т1.13, Т1.14, Т1.16, Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.15 |
| Преступные группы (криминальные структуры) | Использование уязвимостей ПО, архитектуры и конфигурации систем и сетей | Т1.3, Т1.5, Т1.6, Т1.11, Т1.12, Т1.13, Т1.14, Т1.16, Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.15 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

ПРИЛОЖЕНИЕ № 3 – Перечень тактик и соответствующих им техник, используемых для построения сценариев реализации угроз безопасности персональных данных

|  |  |  |
| --- | --- | --- |
| **№** | **Тактика** | **Основные техники** |
| Т1 | Сбор информации о системах и сетях.  Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации | T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций. |
| T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.  Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок. |
| Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей. |
| Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.  Пример: сканирование при помощи сканера nmap. |
| Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.  Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера. |
| Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.  Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера. |
| Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking. |
| Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера. |
| Т1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.  Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства. |
| Т1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы). |
| Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга. |
| Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами. |
| Т1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения. |
| Т1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации. |
| Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках. |
| Т1.16. Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров. |
| Т1.17. Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах. |
| Т1.18. Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах. |
| Т1.19. Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах. |
| Т1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах. |
| Т2 | Получение первоначального доступа к компонентам систем и сетей.  Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий | Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет).  Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации |
| Т2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.  Примеры 1) доступ к датчикам автономной системы дистанционного контроля давления газа участка газопровода; 2) доступ к умному счетчику, расположенному на частном объекте, как к части инфраструктуры поставщика электроэнергии; 3) доступ к интерфейсу управления камеры видеонаблюдения через сети ближнего действия. |
| Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.  Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации. |
| Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке. |
| Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.  Примеры: 1) эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; 2) эксплуатация уязвимостей операционной системы устройства человеко-машинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устройстве паролей доступа; 3) эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта. |
| Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок. |
| Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.  Примеры: 1) передача флеш-носителя в комплекте материалов выездного мероприятия; 2) подмена USB-адаптера беспроводной клавиатуры схожим внешне, но реализующим функции сбора и передачи данных устройством. |
| Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы. |
| Т2.9. Несанкционированное подключение внешних устройств.  Пример: несанкционированное подключение точки доступа Wi-Fi. |
| Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими). |
| Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд). |
| Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа.  Пример: использование доступа третьей доверенной стороны (поставщики ИТ-услуг, поставщики услуг безопасности). |
| Т2.13. Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки. |
| Т2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации.  Пример: демонстрация фотографии для аутентификации через функцию распознавания лиц. |
| Т3 | Внедрение и исполнение вредоносного программного обеспечения в системах и сетях.    Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его программную среду инструментальные средства, необходимые ему для дальнейших действий. | Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии. |
| Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей. |
| Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение. |
| Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами. |
| Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution). |
| Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных. |
| Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.  Примечание 3: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.  Примечание 4: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения. |
| Т3.9. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.  Примечание 5: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения. |
| Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах  Примечание 6: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения. |
| Т3.11. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами. |
| Т3.12. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы. |
| Т3.13. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы. |
| Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п. |
| Т3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии. |
| Т3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL.  Примеры: 1) запуск MSI-файлов в операционной системе Windows при помощи утилиты msiexec; 2) использование утилит Regsvr32.exe (Microsoft Windows RegisterServer) и odbcconf.exe для проксирования исполнения кода библиотек dll в операционной системеWindows посредством внесения изменений в реестр операционных систем. |
| Т4 | Закрепление (сохранение доступа) в системе или сети.  Тактическая задача: получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия). | Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных. |
| Т4.2. Использование штатных средств удаленного доступа и управления операционной системы. |
| Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода. |
| Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки). |
| Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети. |
| Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков. |
| Т4.7. Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей. |
| Т5 | Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ.    Тактическая задача: внедрив вредоносное программное обеспечение или обеспечив постоянное присутствие на узле сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации. | Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования.  Пример: использование средств удаленного управления RMS/teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников. |
| Т5.2. Использование штатных средств удаленного доступа и управления операционной системы. |
| Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.). |
| Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств. |
| Т5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах. |
| Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения.  Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет, в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос. |
| Т5.7. Туннелирование трафика управления через VPN. |
| Т5.8. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие. |
| Т5.9. Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети. |
| Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления. |
| Т5.11. Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п. |
| Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п. |
| T5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения. |
| Т6 | Повышение привилегий по доступу к компонентам систем и сетей.    Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом. | Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими. |
| Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи. |
| Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий.  Пример: эксплуатация уязвимости драйвера службы печати, позволяющей выполнить код с привилегиями системной учетной записи, через доступ к этому драйверу из приложения, запущенного от имени непривилегированного пользователя. |
| Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи).  Пример: эксплуатация уязвимости штатного механизма имперсонации, реализуемого операционной системой. |
| Т6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций.  Пример: кража и подделка cookie сессии для получения авторизованного доступа к вебинтерфейсу управления сетевого устройства. |
| Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима.  Пример: обход UserAccountControl в операционной системе Windows. |
| Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями.  Примеры: 1) использование профилей PowerShell для закрепления ВПО в системе и выполнения этого ПО с повышенными привилегиями; 2) конфигурация команды перехода в привилегированный режим sudo, при которой успешный результат выполнения этой команды на некоторое время кэшируется, что при определенных обстоятельствах может быть использовано вредоносным кодом для выполнения привилегированных операций в течение этого времени; 3) параметры исполнения файлов (ImageFileExecutionOptions, IFEO), позволяющие переключать исполнение файлов в режим отладки, выполняя вредоносные приложения под видом отладчиков и средств мониторинга, что позволяет им отключать системные приложения и средства защиты. |
| Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей.  Пример: подмена на диске бинарных файлов или скриптов, предназначенных для исполнения в привилегированном контексте, приложением, исполняющимся в непривилегированном контексте. |
| Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды.  Пример: эксплуатация уязвимости обработки буфера данных в рамках песочницы, реализуемой браузером для ограничения работы мобильного кода (Javascript), с последующим выполнением кода в контексте процесса браузера. |
| Т7 | Сокрытие действий и применяемых при этом средств от обнаружения    Тактическая задача: нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их. | Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения.  Пример: использование популярной утилиты PsExec для ОС Windows как администраторами, так и нарушителями. |
| Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей. |
| Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей. |
| Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов. |
| Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса. |
| Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности. |
| Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных. |
| Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки. |
| Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей.  Примечание 11: Сочетается с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения. |
| Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе.  Пример: внесение изменений в модули и конфигурацию ВПО для удаления индикаторов компрометации этим ВПО после обнаружения его в других системах. |
| Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности.  Примеры: 1) сокрытие окна приложения через параметры запуска процесса в ОС Windows; 2) выбор для вредоносного приложения имени файла (процесса), похожего на имя известного и/или системного приложения или совпадающего с ним. |
| Т7.13. Создание скрытых файлов, скрытых учетных записей. |
| Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов. |
| Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки. |
| Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки.  Пример: распространение ВПО единовременно по всем интересующим злоумышленникам системам и единовременный запуск его на выполнение по команде, вплоть до выполнения которой компрометацию системы обнаружить сложно. |
| Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода ВПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети. |
| Т7.18. Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе. |
| Т7.19. Туннелирование трафика управления через VPN. |
| Т7.20. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие. |
| Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами. |
| Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков. |
| Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе.  Примечание 12: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.  Примечание 13: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.  Примечание 14: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах.  Примечание 15: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО. |
| Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами. |
| Т7.28. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы. |
| Т7.29. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы. |
| Т8 | Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям.    Тактическая задача: получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей. | Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа. |
| Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям. |
| Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования.  Пример: распространение вредоносного кода групповыми политиками ActiveDirectory, обычно используемыми для автоматического управления легитимным программным обеспечением. |
| Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям. |
| Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами. |
| Т8.6. Копирование вредоносного кода на съемные носители. |
| Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети. |
| Т8.8. Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях.  Пример: отсылка сообщений корпоративной электронной почты от имени коллег и прочих доверенных лиц. |
| Т9 | Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз.  Тактическая задача: в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия | Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования.  Пример: использование средств удаленного управления RMS / teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников. |
| Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы. |
| Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.). |
| Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств. |
| Т9.5. Отправка данных по известным протоколам управления и передачи данных. |
| Т9.6. Отправка данных по собственным протоколам. |
| Т9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения.  Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос. |
| Т9.8. Туннелирование трафика передачи данных через VPN. |
| Т9.9. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие. |
| Т9.10. Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах. |
| Т9.11. Отправка данных через альтернативную среду передачи данных.  Пример: вывод конфиденциальной информации через субтитры видеоряда, демонстрируемого на веб-сайте. |
| Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации. |
| Т9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей. |
| Т9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети). |
| Т10 | Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям.    Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий. | Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках. |
| Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа. |
| Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения. |
| Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения. |
| Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения. |
| Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства. |
| Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей. |
| Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей. |
| Т10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости). |
| Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети. |
| Т10.11. Нецелевое использование ресурсов системы.  Примеры: 1) организация майнинговой платформы; 2) организация платформы для осуществления атак отказа в обслуживании на смежные системы и сети. |
| Т10.12. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов.  Примеры: 1) воздействие на автоматизированные системы управления объектов транспорта; 2) удаленное воздействие на цифровые системы и первичное оборудование объектов электроэнергетики; 3) воздействие на системы управления технологическим процессом нефтехимического объекта. |
| Т10.13. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов. |
| Т10.14. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов. |
| Т10.15. Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой.  Примеры: 1) нанесение нелегитимной разметки дорожного полотна с целью вызова сбоя системы автоматического управления автомобилем; 2) использование специальных символов в идентификационном знаке физического объекта, распознаваемом камерами видеонаблюдения. |

ПРИЛОЖЕНИЕ № 4 – Актуальные уязвимости ИСПДн ООО «111»

| **Наименование уязвимости** | **Описание уязвимости** | **Версия уязвимого ПО** | **Рекомендации по устранению** |
| --- | --- | --- | --- |
| BDU:2022-0573 | Уязвимость реализации протокола Internet Key Exchange (IKE) операционных систем Windows, позволяющая нарушителю выполнить произвольный код | Server 2008 R2 SP1  7 SP1  Server 2008 SP2  8.1  Server 2012 | Установка обновлений из доверенных источников.  В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.  Компенсирующие меры:  - отключение службы IPSec;  - использование средств межсетевого экранирования с целью фильтрации IKEv1-пакетов.  Использование рекомендаций:  https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34722 |
| Уязвимость реализации протокола Internet Key Exchange (IKE) операционных систем Windows связана с ошибками при обработке входных данных. Эксплуатация уязвимостей может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных IKEv1-пакетов |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
|  |
|  |  |  |  |
|  |