МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

# 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура – совокупность основных структурно-функциональных характеристик, свойств, компонентов, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов и не включена оператором системы или сети в границу процесса оценки угроз безопасности информации.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

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

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

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информация – данные, содержащиеся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент – программное, программно-аппаратное или техническое средство.

Контролируемая зона – пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

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

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

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

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

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

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

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

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

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

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

Программное обеспечение – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средство защиты информации (СЗИ) – техническое, программное, программнотехническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

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

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

# 2. ОБЩИЕ ПОЛОЖЕНИЯ

## 2.1. Введение

Настоящая модель угроз безопасности информации (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.

Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в ОРГАНИЗАЦИИ (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в ОРГАНИЗАЦИИ информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования ОРГАНИЗАЦИИ.

## 2.2. Оцениваемые угрозы

Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей. При этом в настоящей Модели угроз не рассматриваются угрозы...

## 2.3. Ответственность за обеспечение защиты информации (безопасности)

Ответственными за обеспечение информационной безопасности ОРГАНИЗАЦИИ приказом РУКОВОДИТЕЛЯ назначены должностные лица / подразделения, представленные в таблице 1.

Таблица 1. Ответственные за обеспечение информационной безопасности

|  |  |  |
| --- | --- | --- |
| № п/п | Роль подразделения / должностного лица | Должностное лицо / подразделение |
| 1 | Пример: Ответственный за обеспечение безопасности | Пример: Руководитель отдела средств защиты |

## 2.4. Особенности пересмотра Модели угроз

Настоящая Модель угроз может быть пересмотрена:

– по решению ОРГАНИЗАЦИИ на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений ОРГАНИЗАЦИИ;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности информации;

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ОРГАНИЗАЦИИ;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в ОРГАНИЗАЦИИ и (или) взаимодействующих (смежных) системах.

# 3. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

## 3.1 Общее описание объекта оценки угроз

Настоящая Модель угроз разработана в отношении ОРГАНИЗАЦИИ.

Основные характеристики ОРГАНИЗАЦИИ:

Состав обрабатываемой информации:

– Пример: Персональные данные

Основные процессы (бизнес-процессы):

– Пример: Осуществление образовательной деятельности (Предполагает организацию и ведение образовательной деятельности в соответствии с законодательством).

Уровень защищенности ПДн:

## 3.2. Состав и архитектура объекта оценки

Состав ОРГАНИЗАЦИИ определен в таблице 2.

Таблица 2. Состав ОРГАНИЗАЦИИ

|  |  |  |
| --- | --- | --- |
| № п/п | Характеристика | Значение характеристики |
| 1 | Программно-аппаратные средства | Сервер с веб-страницей – 1 Сервер обработки данных – 1 Бухгалтерия ПК – 1 Информационная безопасность ПК – 2 Cisco роутер – 3 База данных Postgres – 1 |
| 2 | Общесистемное программное обеспечение | Пример: Операционные системы: - Debian GNU/Linux; - Microsoft Windows Server 2019 Standart, русская версия; - Microsoft Windows Server 2012 R2 Standart x64; - Microsoft Windows 10 Pro, 64-разрядная |
| 3 | Прикладное программное обеспечение | Пример: - 1С Бухгалтерия |
| 4 | Средства защиты информации | Пример: Средства антивирусной защиты: Kaspersky Endpoint Security для Windows (версия 11.1.1.126) Средства криптографической защиты информации: Программный комплекс ViPNet Client 4 (версия 4.5) |

Организация представляет собой локальную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в пределах одного здания (нескольких близко расположенных зданий) и объединенных в единую систему).

Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – присутствует, в соответствии с таблицей 3.

Таблица 3. Подключения к сетям электросвязи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Категория сети электросвязи | Наименование оператора связи | Цель взаимодействия с сетью электросвязи | Способ взаимодействия с сетью электросвязи |
| 1 | Общего пользования | ПАО КОМПАНИЯ | Оказание услуг | Тип доступа: проводной, беспроводной. Протоколы: HTTP, POP3, FTP, SMTP, IMAP4, TCP/IP |

Подключение к информационно-телекоммуникационным сетям – отсутствует/присутствует.

Подключение к информационно-телекоммуникационной сети «Интернет» – отсутствует/присутствует.

Подключение к информационно-телекоммуникационным сетям иных организаций – отсутствует/присутствует.

В ОРГАНИЗАЦИИ не осуществляется/осуществляет взаимодействие с системами и сетями других организаций.

В ОРГАНИЗАЦИИ не осуществляется/осуществляет взаимодействие с другими системами и сетями ОРГАНИЗАЦИИ.

К информационным ресурсам ОРГАНИЗАЦИИ не осуществляется/осуществляет локальный доступ.

К информационным ресурсам ОРГАНИЗАЦИИ не осуществляется/осуществляет удаленный доступ.

Технологии, используемые в ОРГАНИЗАЦИИ отражены в таблице 4.

Таблица 4. Технологии, используемые в ОРГАНИЗАЦИИ

|  |  |  |
| --- | --- | --- |
| № п/п | Технология | Использование |
| 1 | Съемные носители информации | Не используются |
| 2 | Технология виртуализации | Используются |
| 3 | Технология беспроводного доступа |  |
| 4 | Мобильные технические средства |  |
| 5 | Веб-серверы |  |
| 6 | Технология веб-доступа |  |
| 7 | Smart-карты |  |
| 8 | Технологии грид-систем |  |
| 9 | Технологии суперкомпьютерных систем |  |
| 10 | Большие данные |  |
| 11 | Числовое программное оборудование |  |
| 12 | Электронная почта |  |
| 13 | Технология передачи видеоинформации |  |
| 14 | Технология удаленного доступа |  |
| 15 | Технология удаленного внеполосного доступа |  |
| 16 | Технология искусственного интеллекта |  |

# 4. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

Негативные последствия определяются применительно к нарушению основных (критических) процессов (бизнес-процессов) ОРГАНИЗАЦИИ и применительно к нарушению безопасности информации.

На основе анализа исходных данных ОРГАНИЗАЦИИ определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 5.

Таблица 5. Виды рисков (ущерба) и негативные последствия

|  |  |  |
| --- | --- | --- |
| Иденти- фикатор | Негативные последствия | Вид риска (ущерба) |
| НП.1 | Разглашение персональных данных граждан | Ущерб физическому лицу |
| НП.2 | Нарушение неприкосновенности частной жизни | Ущерб физическому лицу |
| НП.3 | Нарушение личной, семейной тайны, утрата чести и доброго имени | Ущерб физическому лицу |
| НП.4 | Нарушение конфиденциальности (утечка) персональных данных | Ущерб физическому лицу |
| НП.5 | Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель) | Ущерб юридическому лицу |
| НП.6 | Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций | Ущерб юридическому лицу |
| НП.7 | Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) | Ущерб юридическому лицу |
| НП.8 | Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) | Ущерб юридическому лицу |

# 5. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты ОРГАНИЗАЦИИ, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, определенным в разделе 4 настоящей Модели угроз, – объектов воздействия.

Объекты воздействия определялись для реальной архитектуры и условий функционирования ОРГАНИЗАЦИИ на основе анализа исходных данных и проведенной инвентаризации.

Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 6.

Таблица 6. Виды воздействия

|  |  |
| --- | --- |
| Иденти- фикатор | Вид воздействия |
| ВВ.1 | Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности) |
| ВВ.2 | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным |
| ВВ.3 | Отказ в обслуживании компонентов (нарушение доступности) |
| ВВ.4 | Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) |
| ВВ.5 | Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач |
| ВВ.6 | Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации |

Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 7.

Таблица 7. Объекты воздействия и виды воздействия

|  |  |  |
| --- | --- | --- |
| Негативные последствия | Объекты воздействия | Виды воздействия |
| Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций | Рабочая станция | ВВ.1 ВВ.2 ВВ.4 ВВ.5 |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) | Виртуальная машина | ВВ.1 ВВ.3 ВВ.4 ВВ.6 |
| Нарушение личной, семейной тайны, утрата чести и доброго имени | Рабочая станция | ВВ.1 ВВ.2 ВВ.4 ВВ.5 |

# 6. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

## 6.1. Антропогенные источники

В ходе оценки угроз безопасности информации определяются возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие(ая) реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты ОРГАНИЗАЦИИ.

Формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предположений об их отнесении к числу возможных нарушителей (нарушителей, подлежащих дальнейшей оценке), представлены в таблице 8.

Таблица 8. Перечень рассматриваемых нарушителей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нарушителя | Возможные цели реализации угроз безопасности информации | Актуальность возможных нарушителей |
| 1 | Специальные службы иностранных государств | Нанесение ущерба государству в области обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций; Получение конкурентных преимуществ на уровне государства; Срыв заключения международных договоров; Создание внутриполитического кризиса | Актуально/ Не актуально (причина) |
| 2 | Террористические, экстремистские группировки | Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций | Актуально/ Не актуально (причина) |
| 3 | Преступные группы (криминальные структуры) | Получение финансовой или иной материальной выгоды; Желание самореализации (подтверждение статуса) | Актуально/ Не актуально (причина) |
| 4 | Отдельные физические лица (хакеры) | Получение финансовой или иной материальной выгоды;Любопытство или желание самореализации (подтверждение статуса) | Актуально/ Не актуально (причина) |
| 5 | Конкурирующие организации | Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ | Актуально/ Не актуально (причина) |
| 6 | Разработчики программных, программно-аппаратных средств | Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия | Актуально/ Не актуально (причина) |
| 7 | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия | Актуально/ Не актуально (причина) |
| 8 | Поставщики вычислительных услуг, услуг связи | Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия | Актуально/ Не актуально (причина) |
| 9 | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия | Актуально/ Не актуально (причина) |
| 10 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора | Получение финансовой или иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия | Актуально/ Не актуально (причина) |
| 11 | Авторизованные пользователи систем и сетей | Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия | Актуально/ Не актуально (причина) |
| 12 | Системные администраторы и администраторы безопасности | Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия | Актуально/ Не актуально (причина) |
| 13 | Бывшие (уволенные) работники (пользователи) | Получение финансовой или иной материальной выгоды; Месть за ранее совершенные действия | Актуально/ Не актуально (причина) |

Проведено определение характеристик (категория нарушителя и уровень возможности по реализации угроз безопасности информации) возможных нарушителей, а также сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации. По результатам сопоставления определяются актуальные нарушители по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ОРГАНИЗАЦИИ негативным последствиям и соответствующим рискам (видам ущерба). Результаты представлены в таблице 9.

Таблица 9. Характеристики актуальных нарушителей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Вид нарушителя | Категория | Уровень возможностей |
| 1 | Отдельные физические лица (хакеры) | Внешний | H1. Нарушитель, обладающий базовыми возможностями |
| 2 | Системные администраторы и администраторы безопасности | Внутренний | Н2. Нарушитель, обладающий базовыми повышенными возможностями |

Категория нарушителя определяется исходя из следующих принципов:

– внешний нарушитель – если нарушитель не имеет прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам ОРГАНИЗАЦИИ, требующим авторизации;

– внутренний нарушитель – если нарушитель имеет права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам ОРГАНИЗАЦИИ. К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ОРГАНИЗАЦИИ.

Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

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

Уровень возможности нарушителя определяется исходя из следующих принципов:

– нарушитель, обладающий базовыми возможностями по реализации угроз безопасности информации – нарушитель имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов;

– нарушитель, обладающий базовыми повышенными возможностями по реализации угроз безопасности информации – нарушитель имеет возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий средними возможностями по реализации угроз безопасности информации – нарушитель имеет возможность реализовывать угрозы, в том числе на выявленные им неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий высокими возможностями по реализации угроз безопасности информации – имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.

# 7. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ОРГАНИЗАЦИИ.

Перечень возможных способов реализации угроз безопасности информации представлен в таблице 10.

Таблица 10. Перечень возможных способов реализации угроз безопасности информации

|  |  |
| --- | --- |
| Идентификатор | Способы реализации |
| СР.1 | Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей) |
| СР.2 | Внедрение вредоносного программного обеспечения |
| СР.3 | Использование недекларированных возможностей программного обеспечения и(или) программно-аппаратных средств |
| СР.4 | Установка программных и(или) программно - аппаратных закладок в программное обеспечение и(или) программно - аппаратные средства |
| СР.5 | Формирование и использование скрытых каналов(по времени, по памяти) для передачи конфиденциальных данных |
| СР.6 | Перехват(измерение) побочных электромагнитных излучений и наводок(других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| СР.7 | Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации |
| СР.8 | Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию) |
| СР.9 | Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств |
| СР.10 | Перехват трафика сети передачи данных |
| СР.11 | Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации |
| СР.12 | Реализация атак типа отказ в обслуживании в отношении технических средств, программного обеспечения и каналов передачи данных |

Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации, включающие описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям, представлены в таблице 11.

Таблица 11. Актуальные способы реализации угроз безопасности информации

|  |  |
| --- | --- |
| Объект взаимодействия | Способы реализации |
| Виртуальная машина | СР.2 |
| Рабочая станция | СР.9 СР.11 СР.2 |

Соотношение актуальных объектов реализации, выявленных у них интерфейсов и способов реализации угроз безопасности информации представлено в таблице 12.

Таблица 12. Возможные способы реализации угроз безопасности на интерфейсах объектов взаимодействия

|  |  |  |
| --- | --- | --- |
| Объекты взаимодействия | Интерфейсы | Способы реализации |
| Виртуальная машина | Каналы удаленного администрирования узла вычислительной сети | СР.9 |
| Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети | СР.5 |

# 8. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для ОРГАНИЗАЦИИ.

Процесс определения актуальных угроз безопасности информации включал:

Выделение из исходного перечня угроз безопасности информации возможных угроз по следующему принципу: угроза безопасности информации признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям:

УБИi = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

Оценку возможных угроз на предмет актуальности по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

Сценарии определяются для соответствующих способов реализации угроз безопасности информации.

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.

Итоговый перечень актуальных угроз безопасности информации представлен в таблице 13.

Таблица 13. Актуальные угрозы безопасности информации

|  |  |  |
| --- | --- | --- |
| Идентификатор угрозы | Наименование угрозы | Характеристика нарушителя, необходимая для реализации угрозы |
| УБИ.213 | Угроза обхода многофакторной аутентификации | Внутренний нарушитель с базовыми возможностями  Внешний нарушитель с высокими возможностями |
| УБИ.001 | Угроза автоматического распространения вредоносного кода в грид-системе | Внутренний нарушитель со средними возможностями  Внешний нарушитель со средними возможностями |
| УБИ.015 | Угроза доступа к защищаемым файлам с использованием обходного пути | Внутренний нарушитель с базовыми повышенными возможностями  Внешний нарушитель с базовыми повышенными возможностями |
| УБИ.002 | Угроза агрегирования данных, передаваемых в грид-системе | Внутренний нарушитель с базовыми возможностями  Внешний нарушитель со средними возможностями |

Соотношение угрозы, объектов, на которые она распространяется, негативных последствий ее реализации, а также способов ее реализации и сценариев представлено в таблице 14.

Таблица 14. Результаты оценки возможных угроз безопасности информации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Идентификатор угрозы | Объекты воздействия | Негативные последствия | Способы реализации угрозы | Возможные сценарии реализации угрозы |
| УБИ.001 | Рабочая станция | НП.3 | СР.2 | -T1.1 -T8.5 |
| УБИ.002 | Рабочая станция | НП.3 | СР.2 | -T1.3 -T7.14 -T7.24 |
| УБИ.015 | Виртуальная машина | НП.8 | СР.2 | -T2.4 -T8.4 |
| УБИ.213 | Рабочая станция | НП.6 | СР.9, СР.11 | -T1.9 -T2.3 -T6.8 |