**Министерство науки и высшего образования РФ**

Федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет»

**(МОСКОВСКИЙ ПОЛИТЕХ)**

**Модель угроз информационной безопасности**

**для информационной системы биометрического**

**терминала банка “Ак Барс” модели СКУД**

Выполнили:

Студенты 3 курса

Группы 181-352

Захаров В.А.

Константинов Д.А.

г. Москва

2021 г.

**Обозначения и сокращения**

|  |  |
| --- | --- |
| АВПО - | антивирусное программное обеспечение |
| АРМ – | автоматизированное рабочее место |
| БД – | база данных |
| ИС – | информационная система |
| КЗ – | контролируемая зона |
| ЛВС – | локально-вычислительная сеть |
| МЭ – | межсетевой экран |
| НДВ – | не декларированные возможности |
| НСД – | несанкционированный доступ |
| ОС – | операционная система |
| ПО – | программное обеспечение |
| ППО – | прикладное программное обеспечение |
| ПТС – | программно-технические средства |
| ПЭМИН – | побочные электромагнитные излучения и наводки |
| РД – | руководящие документы |
| РСБ – | регистрация событий безопасности |
| САВЗ – | средство антивирусной защиты информации |
| СВТ – | средства вычислительной техники |
| СЗ – | система (подсистема) защиты |
| СЗИ – | средства защиты информации |
| СОВ – | система обнаружения вторжений |
| СУБД – | система управления базами данных |
| ТУ – | технические условия |
| УБ – | угрозы безопасности |
| СКЗИ – | средство криптографической защиты информации |
| СКУД – | система контроля и управления доступом |

1. **Термины и определения**

В настоящем документе используются следующие термины и их определения:

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

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**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.

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

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

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

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

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем

присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных** – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

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

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

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

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

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Недекларированные возможности** – функциональные возможности 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.

**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.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – 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 информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или 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.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

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

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

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

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

**Уязвимость** – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

1. **Общие положения**
   1. Разработка модели угроз безопасности информации, обрабатываемой в информационной системе биометрического терминала банка «Ак Барс» (далее – ИС «Ак Барс») проведена в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119;

- Федеральный закон №184-ФЗ "О техническом регулировании".

* 1. Модель угроз безопасности информации, обрабатываемой в ИС «Ак Барс» разработана на основании:

- Методики оценки угроз безопасности информации, утвержденной приказом заместителя директора ФСТЭК от 5 февраля 2021 г.;

- Банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю, расположенной на информационном ресурсе <http://bdu.fstec.ru/threat>;

- Книге “Персональные данные: что было, что будет, на чем сердце успокоится...” под авторством Ксении Шудровой, расположенной на информационном ресурсе http://shudrova.blogspot.com/p/blog-page\_23.html;

* 1. Модель угроз содержит данные по УБ, связанные с:

- Перехватом (съемом) информации по техническим каналам с целью их копирования или неправомерного распространения;

- Несанкционированным, в том числе случайным, доступом в систему с целью нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

* 1. Моделью угроз необходимо руководствоваться на всех этапах жизненного цикла системы: при проектировании, в режиме эксплуатации, при проведении регламентных и ремонтно-профилактических работ, модернизации и выводе ее из эксплуатации.
  2. Частная модель угроз применяется при решении следующих задач:

- Анализа защищенности от угроз безопасности в ходе организации и выполнения работ по обеспечению безопасности;

- Разработки системы защиты, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты;

- Проведения мероприятий, направленных на предотвращение НСД к информации и (или) модификации и блокированию действий лиц, не имеющих права доступа информации;

- Недопущения воздействия на технические средства системы, в результате которого может быть нарушено их функционирование;

- Контроля над обеспечением требований к установленному классу защищенности ИС.

* 1. Угрозы безопасности информации, содержащиеся в настоящей модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности информации в ИС.
  2. Плановый пересмотр проводится с периодичностью не реже чем один раз в 3 года. По результатам анализа проводится уточнение (при необходимости) модели угроз безопасности информации.
  3. Пересмотр (переоценка) угроз безопасности информации осуществляется в случаях:

- изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регла­ментирующих защиту информации;

- изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало воз­никновение новых угроз безопасности информации;

- выявления уязвимостей, приводящих к возникновению новых угроз без­опасности информации или к повышению возможности реализации существую­щих;

- появления сведений и фактов о новых возможностях нарушителей.

* 1. Принципы модели угроз:

- Безопасность персональных данных и иной защищаемой информации при их обработке в информационных системах обеспечивается с помощью системы защиты информации в ИС «Ак Барс».

- При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных и иной защищаемой информации (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

- Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

- Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

- Система защиты информации ИС «Ак Барс» (в том числе и СКЗИ) не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (система защиты информации не предназначена для защиты информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

- Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

- Криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ.

- СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

- Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

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

**3.  Описание ИС Биотерминала «Ак Барс»**

* 1. Общие сведения об информационной системе:
* Сервер ядра ИС:
  1. ЦПУ не менее 8-х;
  2. ОЗУ не менее 8Gb;
  3. Объем жесткого диска не менее 40Gb;
  4. Ubuntu 18.04.5 LTS;
  5. Доступ в глобальную сеть интернет (на момент установки и настройки);
  6. Доступ в локальную сеть
* Сервер локальной части:
  1. ЦПУ не менее 8-х;
  2. ОЗУ не менее 8Gb;
  3. Объем жесткого диска не менее 40Gb;
  4. Ubuntu 18.04.5 LTS;
  5. Доступ в глобальную сеть интернет (на момент установки и настройки);
  6. Доступ в локальную сеть
* Терминал распознавания:
  1. Архитектура NVIDIA
  2. Ubuntu 18.04.5 LTS;
  3. Объем жесткого диска не менее 16Gb;
  4. Доступ в глобальную сеть интернет (на момент установки и настройки);
  5. Доступ в локальную сеть для связи с сервером
  6. Web камера инфракрасная
  7. Стерео камера
  8. Maxwell Процессор ARM
  9. Cortex-A57 MPCore
  10. Оперативная память - 4 Гб
  11. Синхронизированная стерео-камера 1500р
  12. ИК-камера 720р
  13. Подсветка в ИК и оптическом диапазоне
  14. Дисплей 1920\*1080 - Диагональ 7 дюймов
  15. Приложения и компоненты:

ИС «Ак Барс» состоит из десяти приложений и модулей, собственной разработки разделенные на 4 части:

* Сервер ядра ИС:
  1. Abdt.Face2Action. Auth – Сервис авторизации
  2. Abdt.Face2Action.Sync.Matcher – Модуль БД для сравнения эмбедингов
  3. Abdt.Face2Action.Extractor – Приложение для получение эмбедингов с фотографии
  4. Abdt.Face2Action.Server.Sync – Приложение для внесения информации о ФИО и номерах карт СКУД
  5. Abdt.Face2Action.Validator.Server – Приложение для внесения эмбедингов и внесения в БД
  6. Abdt.Face2Pass.Broker – Приложение предоставление информации о пользователе
  7. Abdt.Face2Action.Logger.Server – Приложение для внесения информации о попытках проходов
  8. Abdt.Face2Action.Journal – Приложение получения информации о попытках проходов
  9. Abdt.Face2Action.WebJournal – Веб сайт для отображения информации
* Сервер локальной части:
  1. Abdt.Face2Pass.Validator.Local – Приложение сравнения фотографии полученной с терминала и эмбединга сохраненного в БД
  2. Abdt.Face2Pass.Local.Sync – Приложение получения информации с серверной части в локальную и передачи информации о проходах
  3. Abdt.Face2Action.Extractor – Приложение для получение эмбедингов с фотографии
* Терминал распознавания:
  1. Abdt.Face2Pass.Terminal – Приложение для отображения информации о нахождении сотрудника в БД. Приложение реализовано на архитектуре AARM64 и работает на оборудовании Nvidia Jetson Nano

Для полноценного запуска системы и дальнейшей работы дополнительно будут установлены сторонние программы и компоненты:

* PostgreSQL 11 – база данных;
* Minio s3 – объектное хранилище, для хранения фотографий сотрудников с терминалов;
* Nginx – http сервер;

**4.  Возможности нарушителей (модель нарушителя)**

* 1. В качестве источников угроз несанкционированного доступа к информации при ее обработке в ИС могут выступать лица (нарушители), случайно или преднамеренно совершающие действия, следствием которых может стать нарушение одного из свойств безопасности информации (конфиденци­альности, целостности, доступности).
  2. В настоящем документ представлена лишь часть разработанный модели нарушитель, чтобы ознакомиться с действующей версия следует перейди в EXEL таблицу.
  3. Нарушители подразделяются на два типа в зависимости от возможностей доступа к информационной системе:

- внешние нарушители - лица, не имеющие права доступа к инфор­мационной системе, ее отдельным компонентам и реализующие угрозы безопас­ности информации из-за границ информационной системы;

- внутренние нарушители - лица, имеющие право постоянного или разового доступа к информационной системе или к ее отдельным компонентам.

* 1. Угрозы безопасности информации в информационной системе могут быть реализованы следующими видами нарушителей:

- специальные службы иностранных государств (блоков государств);

- внешние субъекты (физические лица);

- разработчики, производители, поставщики программных, технических и программно-технических средств;

- лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

- пользователи информационной системы;

- системные администраторы;

- бывшие работники (пользователи).

- и тд.

* 1. Предположения о видах нарушителей и их целях (мотивации) реализации угроз безопас­ности информации приведены в таблице 1.

Таблица 1

| № вида | Вид нарушителя | Тип нарушителя | Возможные цели (мотивации) реализации УБ |
| --- | --- | --- | --- |
|  | Специальные службы иностран­ных госу­дарств (бло­ков государств) | Внешний, внутренний | Дискредитация или дестабилизация деятельности предприятия. |
|  | Внешние субъ­екты (фи­зические лица) | Внешний | Идеологические или политиче­ские мотивы. Любопытство или желание са­мореали­зации (подтверждение ста­туса). Выявление уязвимостей с це­лью их дальнейшей продажи и получения фи­нансовой выгоды. |
|  | Разработчики, про­изво­дители про­граммных, тех­нических и про­граммно-техниче­ских средств | Внешний | Внедрение дополнительных функцио­нальных возможностей в ПО или ПТС на этапе разработки. Непреднамеренные, неосто­рожные или неквалифициро­ванные действия. |
|  | Лица, обслужи­вающие ин­фра­структуру опера­тора (администра­ция, охрана, убор­щики и т.д.) | Внутренний | Непреднамеренные, неосто­рожные или неквалифицированные действия. |
|  | Пользователи ин­форма­ционной сис­темы | Внутренний | Любопытство или желание са­мореали­зации (подтверждение ста­туса). Месть за ранее совершенные дейст­вия. Непреднамеренные, неосто­рожные или неквалифициро­ванные действия. |
|  | Системные адми­нистраторы, адми­нистраторы без­опасности | Внутренний | Любопытство или желание са­мореали­зации (подтверждение ста­туса). Месть за ранее совершенные дейст­вия. Выявление уязвимостей с це­лью их дальнейшей продажи и полу­чения иной выгоды. Непреднаме­ренные, неосто­рожные или неквалифи­циро­ванные действия. |
|  | Бывшие работ­ники (пользова­тели) | Внешний | Причинение имущественного ущерба путем мошенничества или иным пре­ступным путем. Месть за ранее совер­шенные действия |

* 1. Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя опреде­ляется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации.

В зависимости от потенциала, требуемого для реализации угроз безопас­ности информации, нарушители подразделяются:

- на нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- на нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- на нарушителей, обладающих высоким потенциалом нападения при реализа­ции угроз безопасности информации в информационной системе.

Потенциал нарушителей и их возможности приведены в таблице 2.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Потенциал нарушителей | Виды нарушите­лей | Возможности по реализации угроз без­опасности информации |
| 1 | Нарушители с базовым (низ­ким) по­тенци­алом | Внешние субъ­екты (физические лица),  лица, об­служи­вающие инфра­структуру опера­тора, пользова­тели информаци­онной системы,  бывшие работ­ники, | Имеют возможность получить инфор­мацию об уязвимостях отдель­ных ком­понент информационной сис­темы, опуб­ликованную в общедос­тупных ис­точниках.  Имеют возможность получить инфор­мацию о методах и средствах реализа­ции угроз безопасности инфор­мации (компьютерных атак), опубликован­ных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализа­ции атак и реализа­цию атак на информационную сис­тему |
| 2 | Нарушители с базовым повышенным (средним) по­тенциалом | Разработчики, про­изводители, поставщики про­граммных, техни­ческих и про­граммно- техниче­ских средств, ад­мини­страторы ин­фор­мационной сис­темы и адми­нист­раторы без­опасно­сти | Обладают всеми возможностями нару­шителей с базовым потенциа­лом.  Имеют осведомленность о мерах за­щиты информации, применяемых в ин­формационной системе данного типа.  Имеют возможность получить инфор­мацию об уязвимостях отдель­ных ком­понент информационной сис­темы пу­тем проведения, с исполь­зованием имеющихся в свобод­ном доступе про­граммных средств, анализа кода при­кладного программного обеспечения и отдель­ных программных компонент общесис­темного программного обеспе­чения.  Имеют доступ к сведениям о струк­турно - функциональных характеристи­ках и особенностях функ­ционирования информационной системы. |
| 3 | Нарушители с высоким по­тенциалом | Специальные службы ино­стран­ных госу­дарств (блоков государств) | Обладают всеми возможностями на­рушителей с базовым и базовым по­вышенным потенциалами.  Имеют возможность осуществлять не­санкционированный доступ из выде­ленных (ведомственных, корпора­тив­ных) сетей связи, к кото­рым возможен физический доступ (незащищенных ор­ганизационными мерами).  Имеют возможность получить дос­туп к системному и при­кладному про­грамм­ному обеспечению, телеком­му­никационному оборудова­нию и другим программно-техниче­ским средствам информационной сис­темы для преднамеренного внесе­ния в них уязвимостей или программ­ных закла­док.  Имеют хорошую осведомленность о мерах защиты информации, применяе­мых в информационной сис­теме, об ал­горитмах, аппаратных и программ­ных средствах, используе­мых в инфор­маци­онной системе. |

* 1. Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного доступа и (или) воздействия на объекты на аппа­ратном уровне;

- несанкционированного доступа и (или) воздействия на объекты на обще­системном уровне (базовые системы ввода-вывода, операционные системы);

- несанкционированного доступа и (или) воздействия на объекты на при­кладном уровне (системы управления базами данных, браузеры, web- приложения, иные прикладные программы общего и специального назначения);

- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства;

- воздействия на пользователей, админи­страторов информационной системы или обслуживающий персонал (социальная инженерия).

- при обработке, включая сбор, биометрических персональных данных на устройстве клиента-физического лица (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения целостности (подмены, удаления) информации о степени соответствия биометрических персональных данных гражданина Российской Федерации).

- при сборе биометрических персональных данных в государственных органах, банках и иных организациях, включая сбор биометрических персональных данных и передачу собранных биометрических персональных данных между структурными подразделениями государственного органа, банка и иной организации ( угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных).

- при передаче собранных биометрических персональных данных между государственным органом, банком, иной организацией и единой биометрической системой (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), угроза нарушения конфиденциальности (компрометации) биометрических персональных данных).

- при обработке информации о степени соответствия в банках (угроза нарушения целостности (подмены, удаления) информации о степени соответствия в банках).

- при передаче информации о степени соответствия между банком и единой биометрической системой (угроза нарушения целостности (подмены, удаления) информации о степени соответствия, угроза нарушения конфиденциальности (компрометации) информации о степени соответствия).

- при обработке, хранении, проверке биометрических персональных данных, обработке и передаче информации о степени соответствия в единой биометрической системе (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения доступности (блокирования передачи) информации о степени соответствия).

* + 1. **Возможные негативные последствия от реализации (возникновения) угроз безопасности информации**

|  |  |  |
| --- | --- | --- |
| Негативные  последствия | Объекты воздействия | Виды воздействия |
| Разглашение  персональных  данных граждан  (У1) | База данных  информационной  системы, содержащая  идентификационную  информацию граждан | Утечка идентификационной информации граждан из базы данных |
| Удаленное  автоматизированное  рабочее место (АРМ)  пользователя | Утечка идентификационной информации граждан с АРМ пользователя |
| Линия связи между  сервером основного  центра обработки  данных и сервером  резервного центра  обработки данных | Перехват информации, содержащей  идентификационную информацию граждан, передаваемой по линиям связи |
| Линия связи между  Биометрических терминалом и сервером  резервного центра  обработки данных | Перехват информации, содержащей  идентификационную информацию граждан, передаваемой по линиям связи |

**Актуальные угрозы безопасности информации**

* + 1. **Определение уровня исходной защищенности информационной системы**

Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС, определяемый экспертным методом. Результаты анализа исходной защищенности приведены в таблице 3.

Таблица 3

| Технические и эксплуатационные характеристики ИС | Уровень защищенности | | |
| --- | --- | --- | --- |
| Высокий | Средний | Низкий |
| 1. По территориальному размещению: | | | |
| распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | + |
| 2. По наличию соединения с сетями общего пользования: | | | |
| ИС, имеющая одноточечный выход в сеть общего пользования; | – | – | + |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: | | | |
| чтение, поиск; | – | – | + |
| запись, удаление, сортировка; | – | – | + |
| модификация, передача | – | – | + |
| 4. По разграничению доступа к персональным данным: | | | |
| ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; | – | – | + |
| 5. По наличию соединений с другими базами персональных данных иных информационных систем: | | | |
| интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | – | – | + |
| 6. По уровню обобщения (обезличивания) ресурсов: | | | |
| ИC, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных) | – | – | + |
| 7. По объему конфиденциальной информации, которая предоставляется сторонним пользователям без предварительной обработки: | | | |
| ИС, предоставляющая часть персональных данных | – | – | + |
| **Характеристики ИС по уровням, %** | **44,44** | **44,44** | **11,11** |

Интегрально по всем техническим и эксплуатационным характеристикам ИС уровень исходной защищенности определяется следующим образом:

* ИС имеет **высокий уровень исходной защищенности**, если не менее 70% характеристик ИС соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу);
* ИС имеет **средний уровень исходной защищенности**, если не выполняются условия по пункту 1 и не менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности;
* ИС имеет **низкий уровень исходной защищенности**, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности каждому уровню исходной защищенности ставится в соответствие числовой коэффициент ***Y1***:

**0** – для высокого уровня исходной защищенности;

**5** – для среднего уровня исходной защищенности;

**10** – для низкого уровня исходной защищенности.

Таким образом, ИС «Ак Барс» имеет низкий уровень исходной защищенности (Y1 = 10), так как не выполняются условия по пунктам 1 и 2.

**Определение вероятности, возможности реализации, опасности и актуальности угроз безопасности информации**

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

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной ИС в складывающихся условиях обстановки. Используем четыре вербальных градации этого показателя:

**маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

**низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

**средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;

**высокая вероятность** – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

Для составления перечня актуальных угроз безопасности каждой градации вероятности возникновения угрозы ставим в соответствие числовой коэффициент Y2:

**0** – для маловероятной угрозы;

**2** – для низкой вероятности угрозы;

**5** – для средней вероятности угрозы;

**10** – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y определяем соотношением:

**Y = (Y1+Y2)/20**.

По значению коэффициента реализуемости угрозы Y формируем вербальную интерпретацию реализуемости угрозы следующим образом:

если **0 ≤ Y ≤ 0.3**, то возможность реализации угрозы признается низкой;

если **0.3 < Y ≤ 0.6**, то возможность реализации угрозы признается средней;

если **0.6 < Y ≤ 0.8**, то возможность реализации угрозы признается высокой;

если **Y > 0.8**, то возможность реализации угрозы признается очень высокой.

Оценка опасности (ущерба) каждой угрозы выполняется экспертным путем, при котором определяется вербальный показатель, имеющий три значения:

**низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям;

**средняя опасность** – если реализация угрозы может привести к негативным последствиям;

**высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность. Решение об актуальности угрозы безопасности информации принимается в соответствии с таб­лицей 4.

Таблица 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |

В качестве исходных данных об угрозах безопасности информации и их характеристиках, используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России, а также иные источники, в том числе опубликованные в общедоступных источниках информации.

Результаты определения вероятности, возможности реализации, опасности и актуальности угроз безопасности информации приведены в EXEL таблице.

* + 1. **Актуальные угрозы, способы противодействия**

В таблице 6 представлены актуальные угрозы безопасности для ИС «Ак Барс», а также способы противодействия им.

Таблица 6

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование угрозы** | **Меры по защите от угроз** | |
| **Организационные** | **Технические** |
| ***1*** | Угроза анализа криптографических алгоритмов и их реализации | Использование актуальных версий сертифицированных средств криптографической защиты информации. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***2*** | Угроза внедрения кода или данных | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***3*** | Угроза воздействия на программы с высокими привилегиями |  | ? |
| ***4*** | Угроза деструктивного изменения конфигурации/среды окружения программ |  | ? |
| ***5*** | Угроза доступа к защищаемым файлам с использованием обходного пути | Информирование пользователей о возможности реализации данной угрозы и вероятными последствиями от ее реализации. | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов |
| ***6*** | Угроза загрузки нештатной операционной системы | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. | Наличие списка разрешенных внешних периферийных устройств |
| ***7*** | Угроза изменения компонентов системы | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. | Наличие в системе функции вычисления контрольной суммы целостности и ее сопоставление с уже имеющейся в системе |
| ***8*** | Угроза искажения вводимой и выводимой на периферийные устройства информации |  | ? |
| ***9*** | Угроза использования информации идентификации/аутентификации, заданной по умолчанию | Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию» | Блокирование встроенных учетных записей с администраторскими правами |
| ***10*** | Угроза использования механизмов авторизации для повышения привилегий |  | ? |
| ***11*** | Угроза использования слабостей протоколов сетевого/локального обмена данными |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***12*** | Угроза неправомерного ознакомления с защищаемой информацией | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. Использова­ние плотных штор или жа­люзи на окнах. Меры по получению доступа в по­меще­ние. Ручная блоки­ровка экрана | Автоматическая блоки­ровка эк­рана по достиже­нии заданного вре­мени не активности. |
| ***13*** | Угроза неправомерных действий в каналах связи |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***14*** | Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика | Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации |
| ***15*** | Угроза несанкционированного доступа к аутентификационной информации |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***16*** | Угроза обхода некорректно настроенных механизмов аутентификации | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***17*** | Угроза перехвата вводимой и выводимой на периферийные устройства информации | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. Использова­ние плотных штор или жа­люзи на окнах. Меры по получению доступа в по­меще­ние. Ручная блоки­ровка экрана | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО |
| ***18*** | Угроза перехвата данных, передаваемых по вычислительной сети |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов |
| ***19*** | Угроза подмены действия пользователя путём обмана | Разработка инструкции по работе в системе, доведение ее до пользователей | Минимизация прав пользователей в системе |
| ***20*** | Угроза подмены доверенного пользователя | Разработка инструкции по работе в системе, доведение ее до пользователей | Минимизация прав пользователей в системе |
| ***21*** | Угроза преодоления физической защиты | Наличие поста охраны, СКУД при входе в организацию, ключевая защита серверной |  |
| ***22*** | Угроза утраты носителей информации | Наличие поста охраны, СКУД при входе в организацию, ключевая защита серверной | Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
| ***23*** | Угроза включения в проект не достоверно испытанных компонентов | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. |  |
| ***24*** | Угроза наличия механизмов разработчика |  | ? |
| ***25*** | Угроза неправомерного шифрования информации |  | Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
| ***26*** | Угроза отказа подсистемы обеспечения температурного режима | Разработка инструкции по действиям сотрудников охраны в случае срабатывания датчика по превышению температуры в серверном помещении | Оснащение серверного помещения основным и резервным кондиционером, установка сигнального датчика и вывод тревожного сигнала на пост охраны здания организации |
| ***27*** | Угроза физического устаревания аппаратных компонентов | Полная ежеквартальная проверка состояния компонентов ИС на их работоспособность | Постоянные мониторинг и тесты аппаратных компонентов |
| ***28*** | Угроза использования уязвимых версий программного обеспечения | Постоянный мониторинг актуальности версий используемого ПО и незамедлительные обновления. |  |
| ***29*** | Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения | Согласно установленной инструкции пользования, советующие обновления происходят в специально выделенные часы работы с 3-5 часов ночи. |  |
| ***30*** |  |  |  |

* + 1. **Способы реализации (возникновения) угроз безопасности информации**

|  |  |  |
| --- | --- | --- |
| * **№** | **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 |
| T1.3. 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 |
| T1.4. 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 |
|  |  | *Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для*  *реализации другой тактики в продолжении атаки* |
| 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 |
| *Примечание 2: Получение доступа может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой*  *системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки* |
| 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 |
| Т3.12. 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 системе  Windows посредством внесения изменений в реестр операционных систем |
| *Примечание 7: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях может выполняться в несколько шагов с использованием одной или более из*  *перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки* |
| 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 |
| *Примечание 8: Закрепление (сохранение доступа в системе) может производиться с*  *использованием одной или более из перечисленных выше техник* |
| 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 веб- интерфейсу 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 вредоносного ПО 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 |
| *Примечание 10: Повышение привилегий по доступу к компонентам систем и сетей может производиться с использованием одной или более из перечисленных выше техник, пока*  *нарушитель не получит достаточно привилегий для реализации другой тактики в продолжении атаки* |
| 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 вредоносного ПО 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 вредоносного ПО 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 вредоносного ПО, 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 |
| *Примечание 16: Сокрытие действий и применяемых при этом средств от обнаружения может производиться с использованием одной или более из перечисленных выше техник для*  *сокрытия разных свидетельств компрометации системы или для более эффективного сокрытия* |
| 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 |
| *Примечание 17: Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для*  *продолжения атаки* |
| 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) |
| *Примечание 18: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз может выполняться с использованием одной или более из перечисленных выше техник*  *для реализации резервных каналов вывода информации* |
| 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 |
| *Примечание 19: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям при реализации угроз безопасности информации или реализации новых угроз, может выполняться с использованием одной или более из перечисленных выше техник для*  *повышения эффективности воздействия с точки зрения нарушителя или для реализации нескольких типов воздействия на атакуемую систему* |