ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Виды нарушений сетевой безопасности

Стандарты сетевой инфраструктуры

- ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
- ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
- ГОСТ Р ИСО/МЭК 27033-4-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности" утвержден приказом Росстандарта от 19 мая 2021 года N 391-ст.
- ГОСТ Р 56045-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности" утвержден приказом Росстандарта от 20 мая 2021 года N 421-ст.

Основные стандарты можно посмотреть на сайте ФСТЭК

https://fstec.ru/en/rss-lenta/113-tekhnicheskaya-zashchita-informatsii/dokumenty/gosudarstvennye-standarty/377-gosudarstvennye-standarty

ГОСТ Р ИСО/МЭК 27033-1-2011

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить процессом, состоящим из этапов:

1. Рассмотрение корпоративной политики информационной безопасности с целью получения подробностей о любых связанных с сетями рисках, которые всегда будут рассматриваться как высокие, и мерах, средствах контроля и управления сетевой безопасностью, которые должны быть реализованы.

Пример:

- главной задачей является доступность определенных видов информации или услуг;
- все соединения с Интернетом должны осуществляться через шлюз безопасности;
- платежное поручение недействительно без цифровой подписи.

2. Определения области/контекста оценка рисков безопасности:

- сбор информации о текущей и (или) планируемой сетевой среде (рассмотрение корпоративной политики информационной безопасности на *предмет формулировок о рисках*: сбор и проверка информации о текущей и (или) планируемой сети (сетях), архитектуре, приложениях, видов соединений и другие характеристики для оценки рисков и определению того, что является возможным с точки зрения специализированной архитектуры/проекта сетевой безопасности).

- сбор информации об угрозах и уязвимостях сетевой инфраструктуры.

ГОСТ Р ИСО/МЭК 27033-1-2011

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить процессом, состоящим из этапов:

3. Идентификация и оценка рисков сетевой безопасности и соответствующих потенциальных областей действия мер и средств контроля и управления:

- осуществление оценки риска сетевой безопасности и проводимой руководством проверки с использованием информации о риске и оценки рисков, связанных с потенциальными нарушениями значимых предписаний и законов, касающихся сетевых соединений, которые определены соответствующими регулирующими или законодательными органами;
- использование установленных потенциальных неблагоприятных влияний на основную деятельность организации, подтверждающих значимость/секретность данных, которые будут храниться или передаваться по сети.

4. Идентификация поддерживающих мер и средств контроля и управления безопасностью - технических и нетехнических - применяемых не только к сетям.

ГОСТ Р ИСО/МЭК 27033-1-2011

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить процессом, состоящим из этапов:

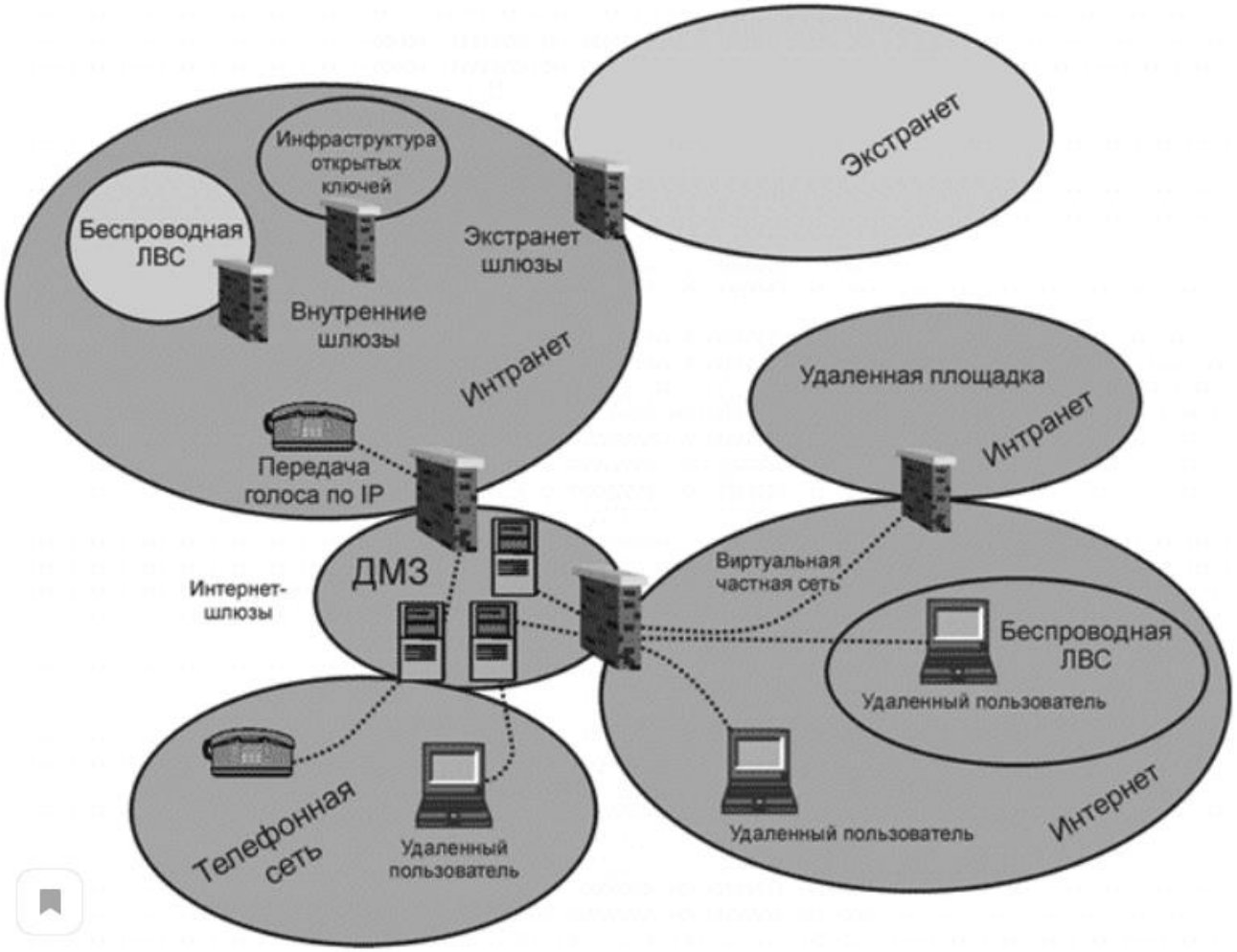
5. Рассмотрение вариантов специализированной архитектуры/проекта сетевой безопасности с учетом сетевых сценариев и вопросов сетевых "технологий", выбором и документированием предпочтительной специализированной архитектуры/проекта безопасности и связанных с ними мер и средств контроля и управления безопасностью.

6. Разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности;

7. Реализация и эксплуатация мер и средств контроля и управления безопасностью;

8. Мониторинг и проверка реализации (мониторинг и проверка мер и средств контроля и управления, необходимых для соблюдения соответствующих предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти).

Пример сетевой среды



ГОСТ Р ИСО/МЭК 27033-1-2011

Оценка риска сетевой безопасности должна проводиться в соответствии с рекомендациями, представленными в ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005. Для этого осуществляется:

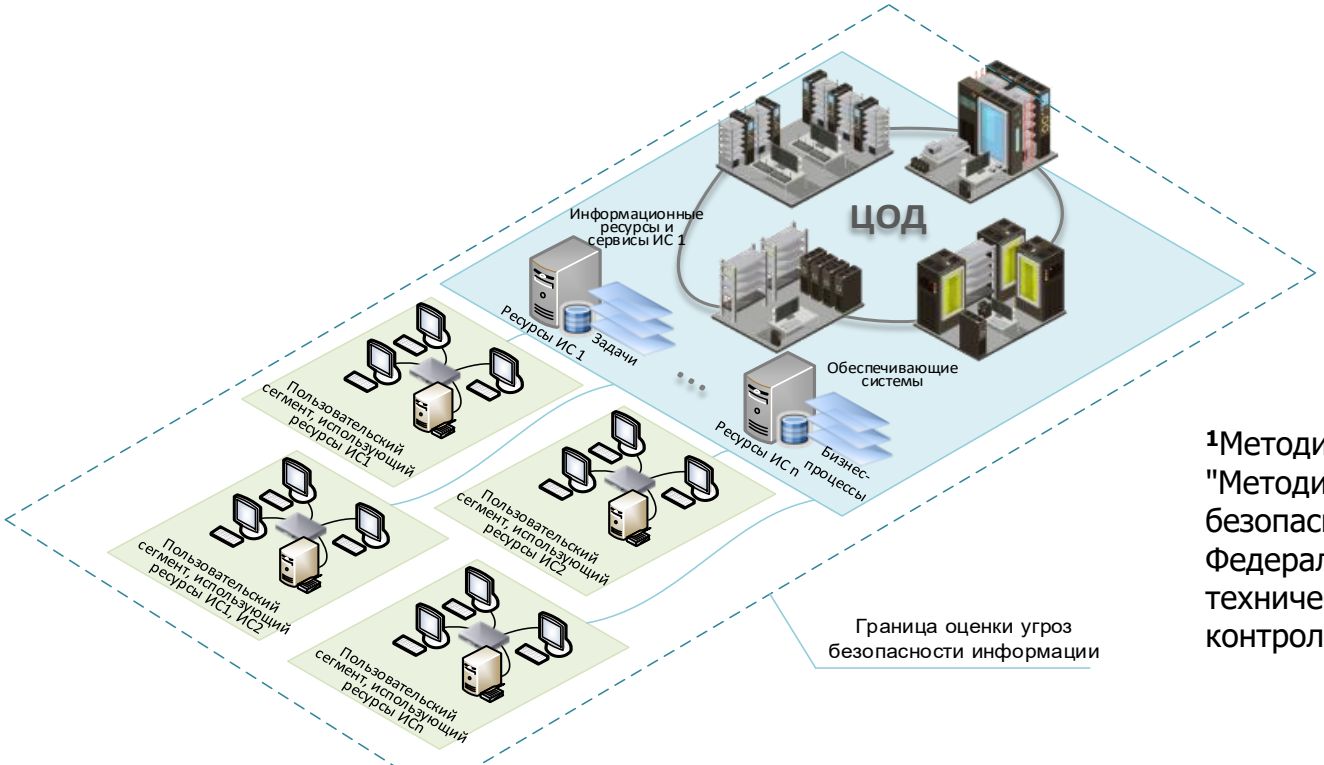
- Определение степени значимости информации и услуг, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность организации в случае возникновения нежелательных инцидентов (оценка активов);
- Идентификация и оценка вероятности или уровней угроз, направленных против информации и услуг;
- Идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;
- Оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на операции деятельности организации и уровнях угроз и уязвимостей;
- идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оцененные риски оставались в допустимых пределах.

ГОСТ Р ИСО/МЭК 27033-1-2011

Оценка угроз[1]

В случае оценки угроз безопасности информации для систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, угрозы безопасности информации определяются как для самих систем и сетей, так и для информационно-телекоммуникационной инфраструктуры, на которой они функционируют.

При размещении систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, принадлежащей поставщику услуг, оценка угроз безопасности информации проводится оператором во взаимодействии с поставщиком услуг



[1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Классификация угроз безопасности информации[1]

По виду каналов, с использованием которых реализуется угроза безопасности информации

Угрозы, реализуемые через каналы возникающие за счёт использования технических средств съёма (добывания) информации, обрабатываемой в технических каналах:

- угрозы утечки информации по логическим каналам связи

- угрозы утечки информации по физическим каналам связи

Угрозы, реализуемые за счёт несанкционированного доступа к данным в с использованием программного обеспечения или специально разрабатываемого программного обеспечения:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения)

- угрозы создания нештатных режимов работы программных средств за счет преднамеренных изменений служебных данных

- угрозы внедрения вредоносных программ (программно-математического воздействия)

[1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Оценка угроз[1]

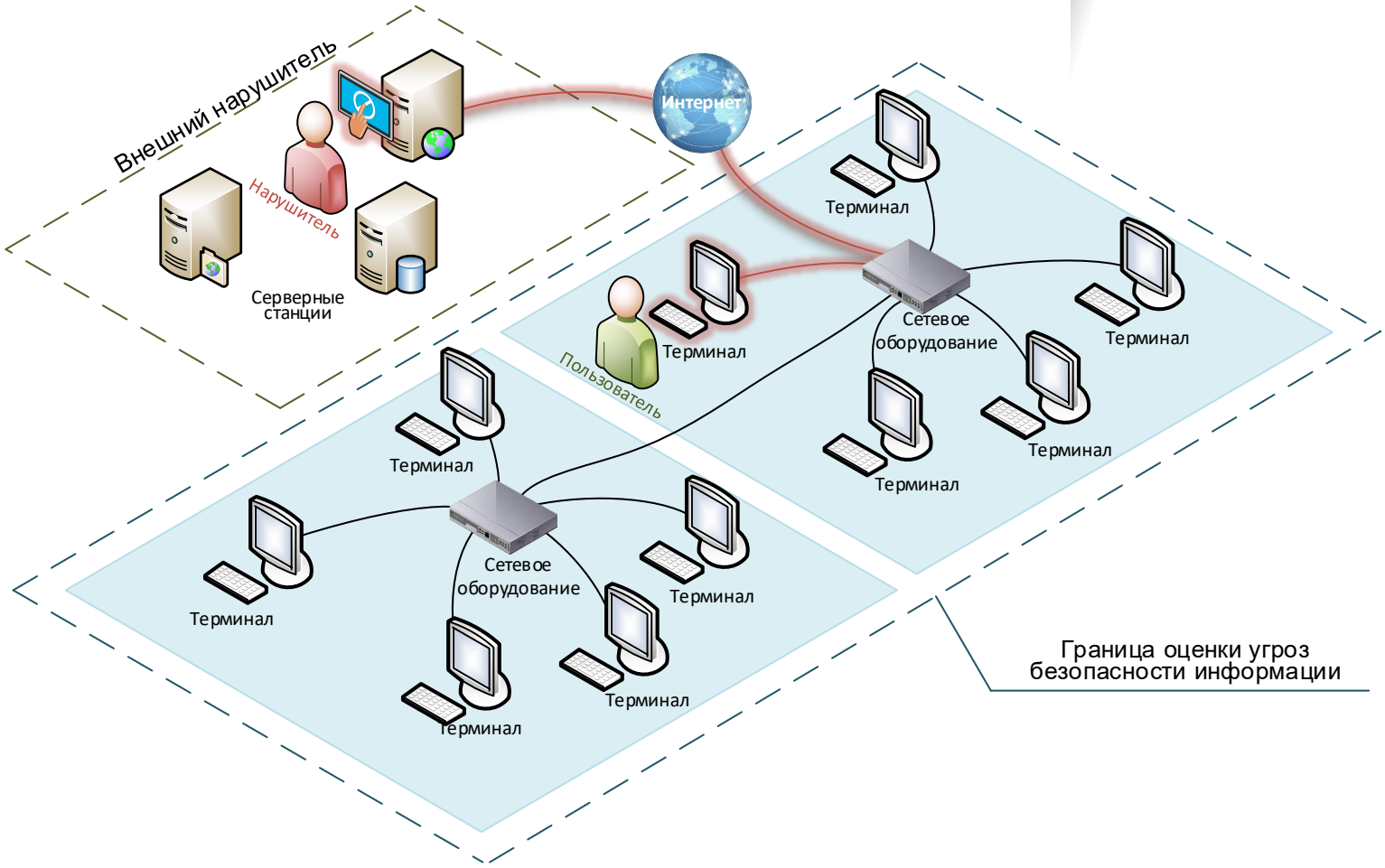
[1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Оценка угроз[1]

Сценарии угроз[1]

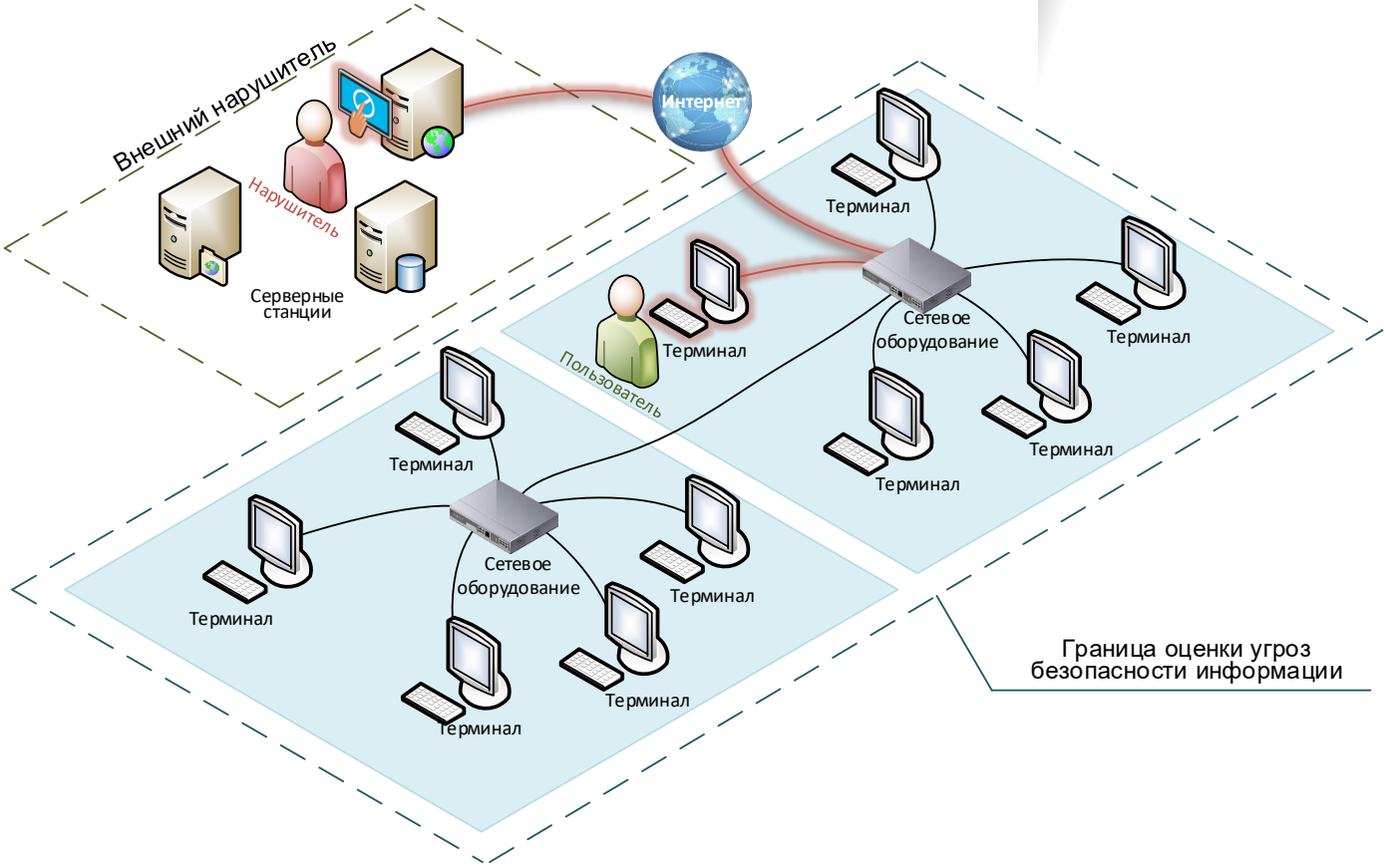
Источник угрозы	Уязвимости	Способ реализации	Объект воздействия	Деструктивное действие
Нарушитель	Уязвимости ПО (наличие вредоносной программы	Использование существующих уязвимостей программно-аппаратного обеспечения КС	Информация, обрабатываемая на хосте	Нарушение конфиденциальности
Программно-аппаратная закладка	Уязвимости, вызванные наличием программно-аппаратной закладки	Внедрение (внесение) новых уязвимостей в КС	Информация в средствах реализующих сетевое взаимодействие	Нарушение целостности (уничтожение, модификация, дезинформация)
Вредоносная программа	Уязвимости, связанные с реализацией сетевых протоколов			
	Уязвимости, вызванные недостатками организации ТЗИ	Уязвимости программно-аппаратных средств в результате сбоев в работе, отказов		Нарушение доступности
	Уязвимости СЗИ			

Определение источника угроз[1]



[1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Определение источника угроз



По результатам определения источников угроз безопасности информации должны быть определены:

а) виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;

б) категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

Элементы описания угроз

- Лица имеющие санкционированный доступ в КС, но не имеющие доступа к ИР
- Зарегистрированный пользователь информационных ресурсов, имеющий ограниченные права доступа в ИС с рабочего места
- Пользователи информационных ресурсов, осуществляющие удалённый доступ по ЛВС
- Зарегистрированный пользователь с полномочиями администратора безопасности
- Зарегистрированный пользователь с полномочиями системного администратора
- Зарегистрированный пользователь с полномочиями администратора безопасности
- Программисты - разработчики прикладного программного обеспечения
- Разработчики и лица обеспечивающие поставку, сопровождение и ремонт технических средств КС
- Другие категории в соответствии с организационной структурой

Пример результата определения актуальных нарушителей при реализации угроз безопасности информации

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности персональных данных граждан; нарушение личной, семейной тайны, утрата чести и доброго имени; финансовый, иной материальный ущерб физических лиц	Преступные группы (криминальные структуры)	Внешний Внутренний***	Н3
		Отдельные физические лица (хакеры)	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н2

Оценка способов реализации угроз. Элементы описания угроз

Уязвимость -недостаток в системе, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу

Ошибки при проектировании и разработке КС

Преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки КС

Неправильные настройки сетевого оборудования, неправомерное изменение режимов работы устройств

Неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ

Внедрение вредоносных программ, создающих уязвимости в сетевом оборудовании

Несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей

Сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

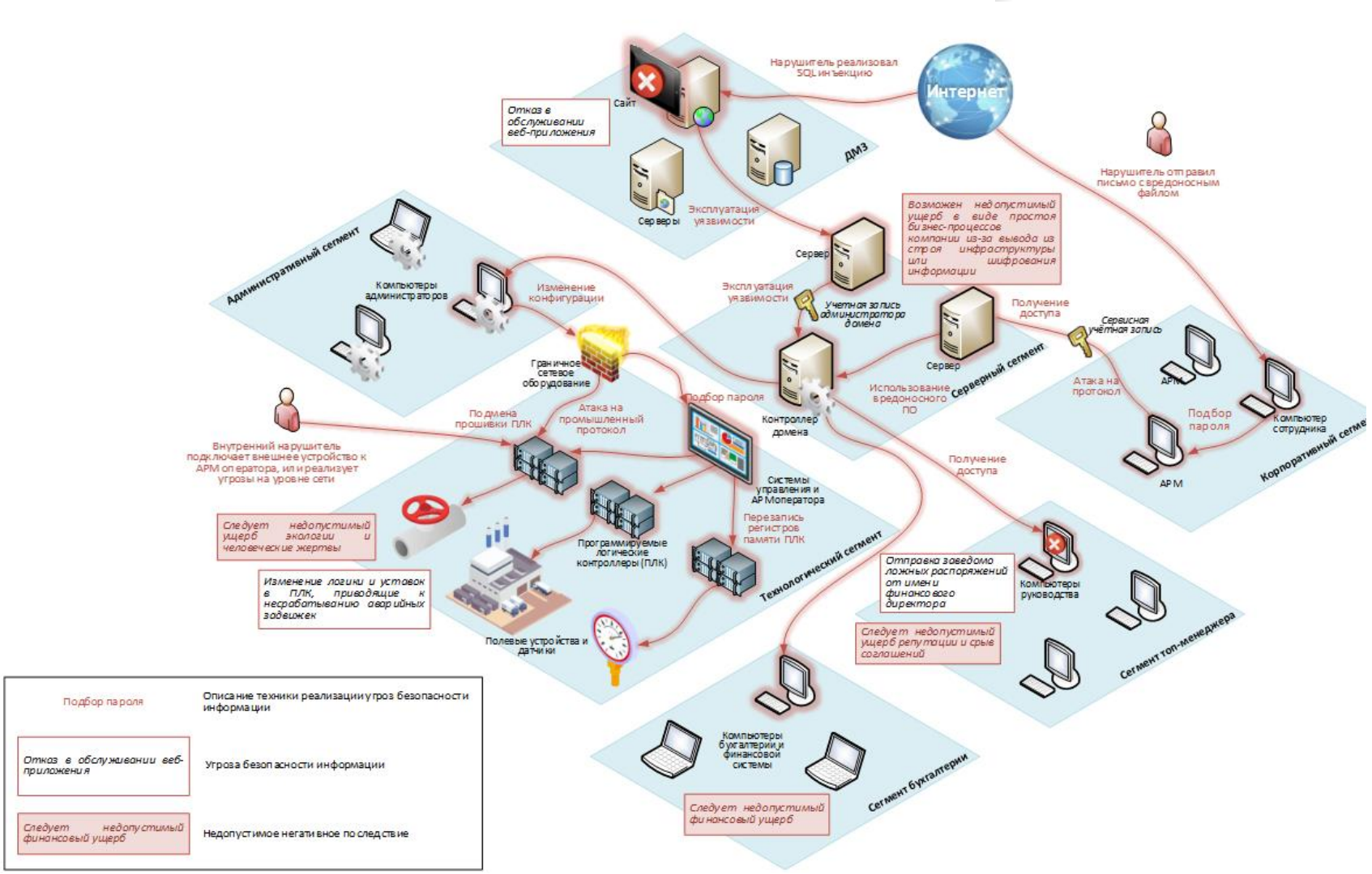
Способ реализации угрозы

- Использование существующих уязвимостей сетевого оборудования и протоколов передачи данных
  - Обход СЗИ
  - Деструктивное воздействие на СЗИ
  - Вскрытие или перехват
- **Уязвимости протоколов сетевого взаимодействия и каналов передачи данных**
  - Перехват информации
  - Модификация передаваемых данных
  - Перегрузка ресурсов (отказ в обслуживании)
  - Внедрение вредоносной программы
  - Удалённый несанкционированный доступ в систему
  - Разглашение и утечка информации на незащищённые хосты
- Использование остаточной, неучтённой информации (сбор «мусора»)
- Использование нетрадиционных каналов передачи данных

- Внедрение (внесение) новых уязвимостей в сетевое оборудование и протоколы передачи данных
  - На этапе проектирования и разработки сети
  - **На этапе эксплуатации**
    - Использование нештатного ПО и оборудования
    - **Внесение уязвимостей с использованием штатных средств**
      - Обмен программами и данными, содержащими выполняемые модули (скрипты, макросы и т.д.)
      - Изменение конфигурации сетевого оборудования
      - Модификация данных
      - Разработка вредоносных программ
      - Публикация, разглашение защищаемых сведений
  - На этапе сопровождения
  - На этапе утилизации

Оценка способов реализации угроз

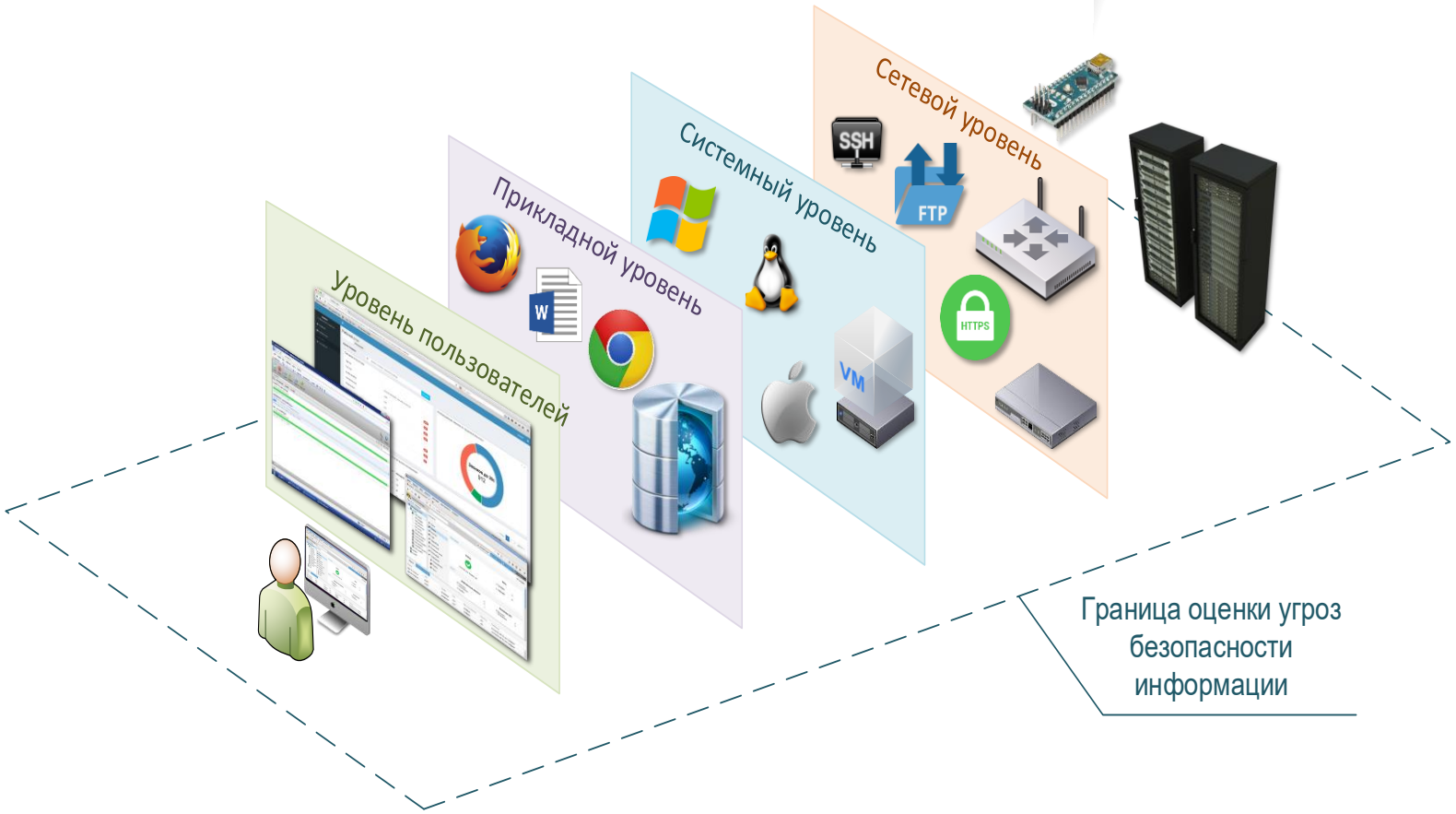
Пример сценариев реализации угроз безопасности информации



Пример основных тактик и соответствующих им типовых техник сценариев угроз

№	Тактика	Основные техники
T1	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

Объекты воздействий



[1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)

Объект воздействия

- Информация обрабатываемая на хосте
  - На отчуждаемых носителях информации
    - Накопители ZIP
    - Накопители электронной памяти типа флэш
    - Сотовые телефоны, карманные компьютеры, цифровые фотоаппараты,mp3- проигрыватели
  - На встроенных носителях долговременного хранения информации
    - Жёсткие магнитные диски
    - Постоянные запоминающие устройства
  - В средствах (портах) ввода/вывода информации
  - В средствах обработки и хранения оперативной информации
    - Оперативная память
      - Кэш-память, буферы ввода-вывода
    - Видео память
      - Оперативная память подключаемых устройств
- Информация в средствах реализующих сетевое взаимодействие и каналах передачи данных в сети
  - Информация на канальном уровне
  - Информация на сетевом уровне
  - Информация на транспортном уровне
  - Информация на сеансовом уровне
  - Информация на презентационном уровне
  - Информация на прикладном уровне
  - Клавиатура
  - Дисплей, монитор
  - Сканер
  - Приводы магнитных и оптических дисков
  - Принтер
  - Плоттер
  - Порты ввода/вывода для подключения периферийных устройств
  - Информация в средствах (аппаратуре) передачи данных
  - Другие средства ввода/вывода информации

Деструктивное действие

- Нарушение конфиденциальности
  - Утечка информации
  - Несанкционированное копирование
  - Перехват информации в каналах передачи данных
  - Разглашение (публикация) защищаемой информации
- Нарушение целостности (уничтожение, модификация, дезинформация)
  - Воздействие на сетевое оборудование и данные
  - Воздействие на микропрограммы, данные и драйвера устройств
  - Воздействия на данные и драйвера устройств обеспечивающие сетевое взаимодействие
  - Воздействие на программы и данные прикладного уровня
  - Внедрение вредоносной программы
  - Внедрение программно-аппаратной закладки
  - Воздействие на СЗИ
  - Воздействие на технологическую сетевую информацию
- Нарушение доступности
  - Нарушение функционирования и отказы средств обработки информации
  - Нарушение и отказы функционирования средств ввода/вывода информации
  - Нарушение и отказы функционирования средств хранения информации
  - Нарушение и отказы функционирования аппаратуры и каналов передачи данных
  - Нарушение и отказы функционирования СЗИ

Средства управления конфигурацией сетей

Средства управления адресами и маршрутизацией передачи данных в сети

Средства управления функциональным контролем сети

Средства управления безопасностью сети

Классификация атак

- Атаки доступа – получение злоумышленником доступа к информации, на которую у него нет прав (доступ к информации, передаваемой по каналам связи).
- Атаки модификации - неправомочное изменение информации (замена, добавление или удаление информации).
- Атаки на отказ в обслуживании (Dos, DDoS) – блокирование использования сервисов системы легальными пользователям (воздействие на среду передачи, необходимую для предоставления сервиса).
- Атаки на отказ от обстоятельств – представлении неверной информации о реальном событии (манипуляции с полем from в адресе электронной почты, IP адресом отправителя).

ГОСТ Р ИСО/МЭК 27033-1-2011

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить следующим образом:

5. Рассмотрение вариантов специализированной архитектуры/проекта сетевой безопасности с учетом сетевых сценариев и вопросов сетевых "технологий", выбором и документированием предпочтительной специализированной архитектуры/проекта безопасности и связанных с ними мер и средств контроля и управления безопасностью;

6. Разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности;

7. Реализация и эксплуатация мер и средств контроля и управления безопасностью;

8. Мониторинг и проверка реализации (мониторинг и проверка мер и средств контроля и управления, необходимых для соблюдения соответствующих предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти).

ГОСТ Р ИСО/МЭК 27033-1-2011

Меры и средства контроля и управления

Для всех сетей должна проводиться проверка соответствия требованиям безопасности по комплексному контрольному перечню, составленному из мер и средств контроля и управления, определенных в:

- политике сетевой безопасности;
- соответствующих SecOPs;
- специализированной архитектуре безопасности;
- политике (безопасности) доступа к сервису шлюза безопасности;
- планах обеспечения непрерывности деятельности;
- условиях обеспечения безопасности соединения (при необходимости).

Литература

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. https://fstec.ru/en/rss-lenta/113-tekhnicheskaya-zashchita-informatsii/dokumenty/gosudarstvennye-standarty/377-gosudarstvennye-standarty
2. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
3. ГОСТ Р ИСО/МЭК 27033-4-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности" утвержден приказом Росстандарта от 19 мая 2021 года N 391-ст.
4. ГОСТ Р 56045-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности" утвержден приказом Росстандарта от 20 мая 2021 года N 421-ст.
5. [1]Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)