Лекция 15. Введение в корпоративные сети

Основные вопросы лекции:

1. Вводные замечания.
2. Интрасети и экстрасети.
3. Уязвимые места сетевой структуры с IP-протоколом.

1. Вводные замечания

1.1. Понятие корпоративной сети

Корпоративная сеть представляет собой совокупность компьютеров, серверов, сетевого оборудования и программных средств, которые объединены для обмена информацией и совместной работы сотрудников организации.

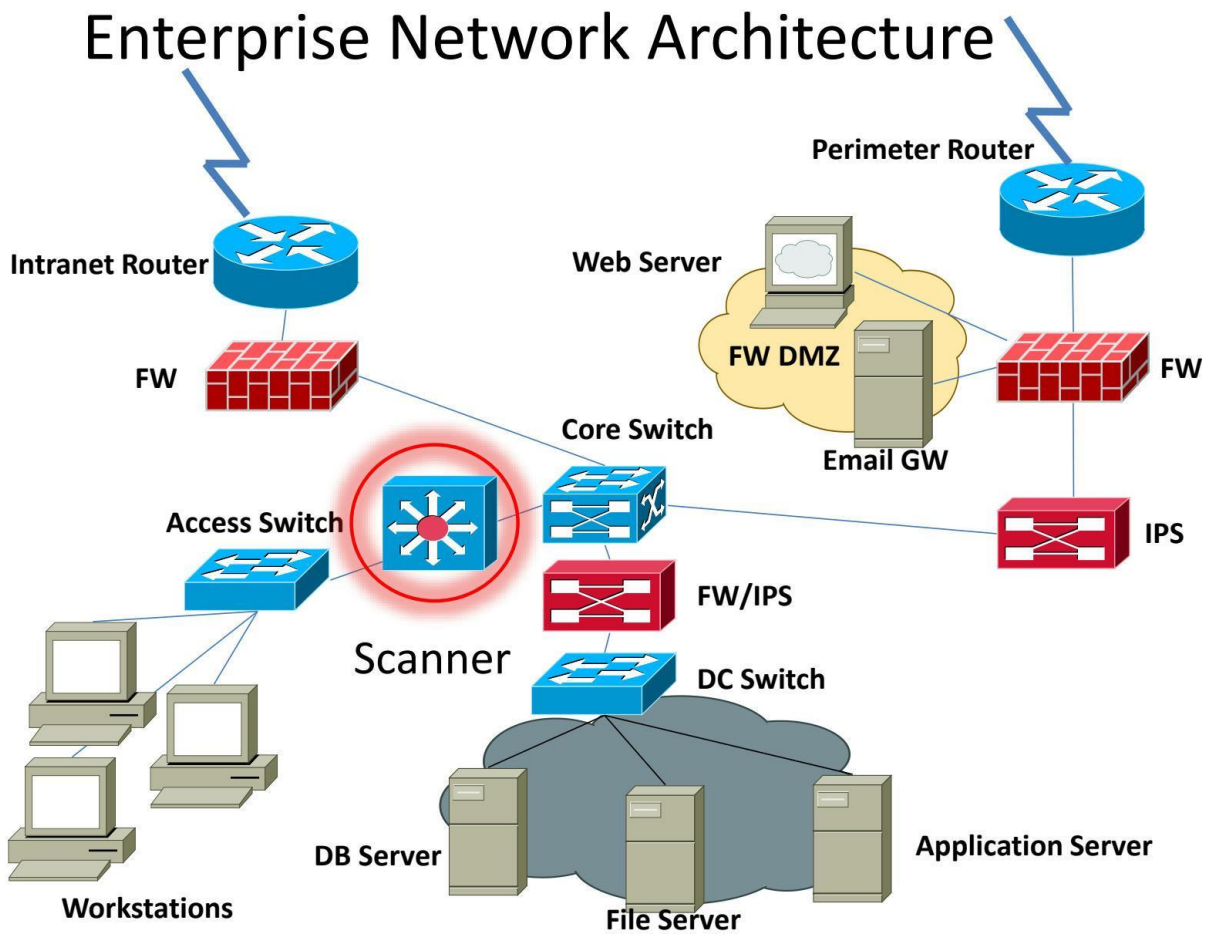
Такая сеть может охватывать один офис, несколько зданий, филиалы в разных городах и даже подразделения в разных странах.

Корпоративная сеть обеспечивает:

- обмен данными между сотрудниками;
- доступ к общим файлам и документам;
- работу с корпоративными информационными системами;
- использование электронной почты и видеосвязи;
- доступ к базам данных;
- взаимодействие с удалёнными подразделениями;
- защиту корпоративной информации.

Пример. В университете корпоративная сеть может объединять учебные корпуса, библиотеку, деканаты, бухгалтерию, компьютерные классы и серверный центр. Сотрудники получают доступ к необходимым ресурсам в соответствии со своими правами.

1.2. Основные компоненты корпоративной сети

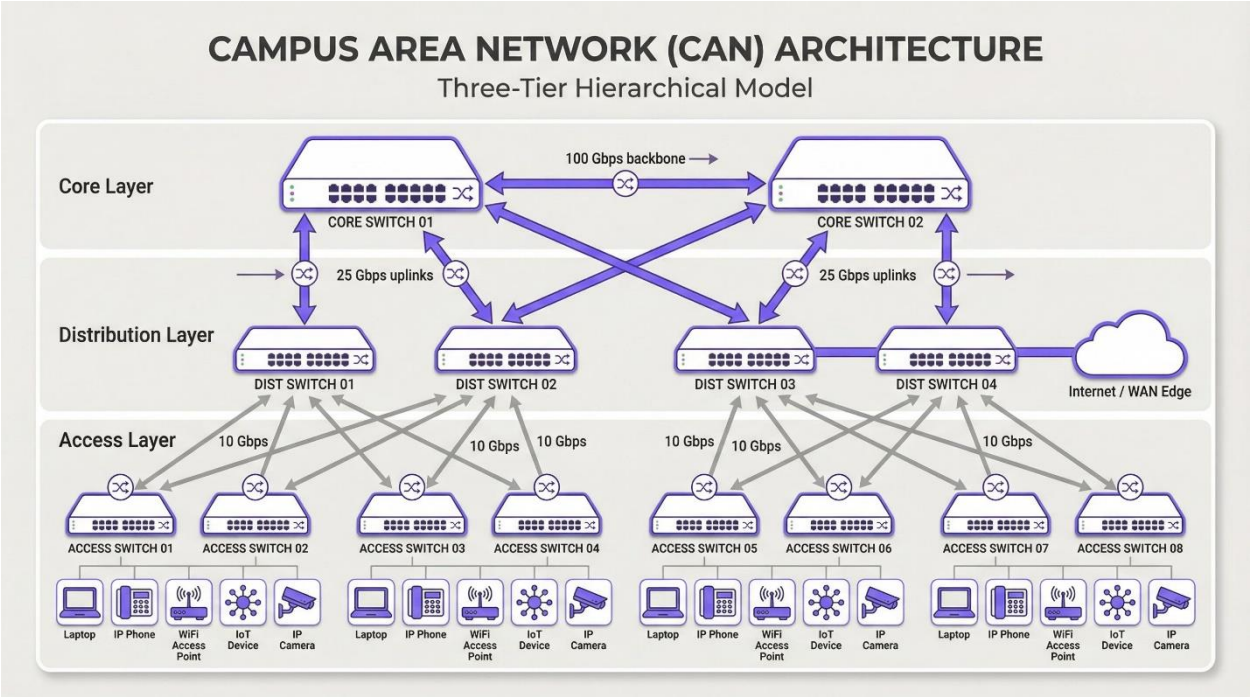


Корпоративная сеть включает несколько основных компонентов.

Компонент	Назначение
Рабочие станции	Компьютеры сотрудников
Серверы	Хранение данных и предоставление сетевых услуг
Коммутаторы	Объединение устройств в локальной сети
Маршрутизаторы	Передача пакетов между сетями
Межсетевые экраны	Контроль и фильтрация сетевого трафика
Точки доступа Wi-Fi	Беспроводное подключение
Каналы связи	Соединение офисов и филиалов
Системы защиты	Контроль доступа и обнаружение атак

1.3. Архитектура корпоративной сети

В корпоративных сетях часто используется иерархическая архитектура. Она состоит из трёх уровней.



1. Уровень доступа (Access Layer).

На этом уровне к сети подключаются конечные устройства:

- компьютеры;
- принтеры;
- IP-телефоны;
- камеры видеонаблюдения;
- точки беспроводного доступа.

2. Уровень распределения (Distribution Layer).

Он объединяет коммутаторы уровня доступа. Здесь могут выполняться:

- маршрутизация между VLAN;
- фильтрация трафика;
- применение правил безопасности;
- управление сетевыми потоками.

3. Ядро сети (Core Layer).

Ядро обеспечивает быструю передачу данных между крупными сегментами корпоративной сети. Оно соединяет серверные центры, уровни распределения и внешние каналы связи.

1.4. Требования к корпоративным сетям

К корпоративным сетям предъявляются следующие требования:

Требование	Содержание
Производительность	Высокая скорость передачи данных
Надёжность	Стабильная работа сетевых устройств и каналов
Безопасность	Защита информации от несанкционированного доступа

Масштабируемость	Возможность подключения новых пользователей и филиалов
Управляемость	Централизованный контроль сетевых ресурсов
Доступность	Возможность работы с ресурсами в необходимое время

Особое значение имеет информационная безопасность. В корпоративной сети могут храниться персональные данные, финансовые документы, сведения о сотрудниках и коммерческая информация.

2. Интрасети и экстрасети

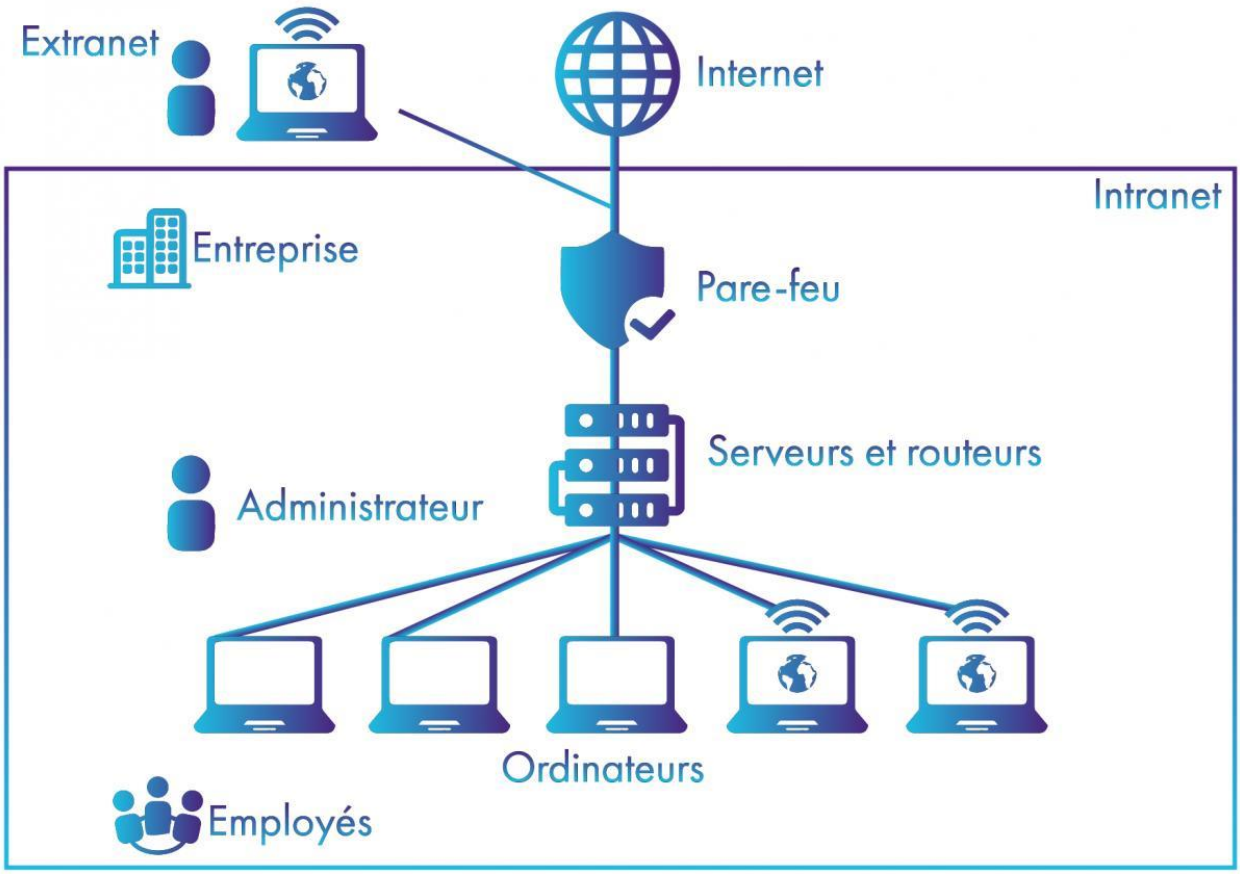
2.1. Понятие интрасети

Интрасеть (Intranet) представляет собой внутреннюю сеть организации, которая использует технологии и протоколы Интернета, но предназначена для сотрудников и других авторизованных пользователей.

Основой интрасети часто выступают:

- протокол TCP/IP;
- веб-серверы;
- браузеры;
- внутренние порталы;
- системы управления документами;
- корпоративные базы данных.

Интрасеть может быть доступна только внутри организации или через защищённое удалённое подключение.



Пример использования интрасети в университете:

- преподаватели получают доступ к учебным материалам;
- студенты просматривают расписание;
- сотрудники работают с внутренними документами;
- администрация использует электронный документооборот;
- руководство получает отчёты из корпоративных баз данных.

2.2. Основные функции интрасети

1. Обмен информацией. Сотрудники получают доступ к общим документам и сообщениям.
2. Совместная работа. Несколько пользователей могут работать с общими материалами.
3. Управление документами. Файлы хранятся в централизованных хранилищах.
4. Доступ к информационным системам. Пользователи работают с бухгалтерскими, кадровыми и учебными программами.
5. Внутренние коммуникации. Используются корпоративные порталы, чаты и электронная почта.

2.3. Понятие экстрасети

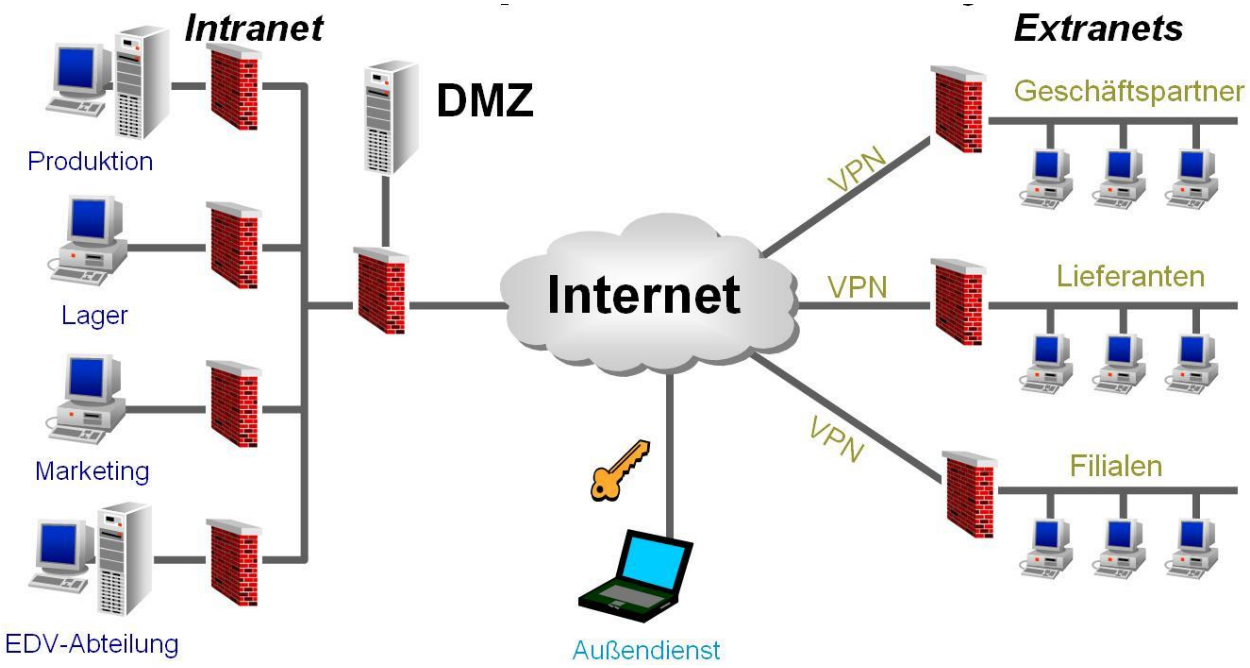
Экстрасеть (Extranet) представляет собой защищённую часть корпоративной сети, к которой предоставляется ограниченный доступ внешним пользователям.

К таким пользователям относятся:

- деловые партнёры;

- поставщики;
- заказчики;
- подрядчики;
- клиенты организации.

Экстрасеть позволяет организации обмениваться информацией с внешними участниками без предоставления им полного доступа к внутренним ресурсам.

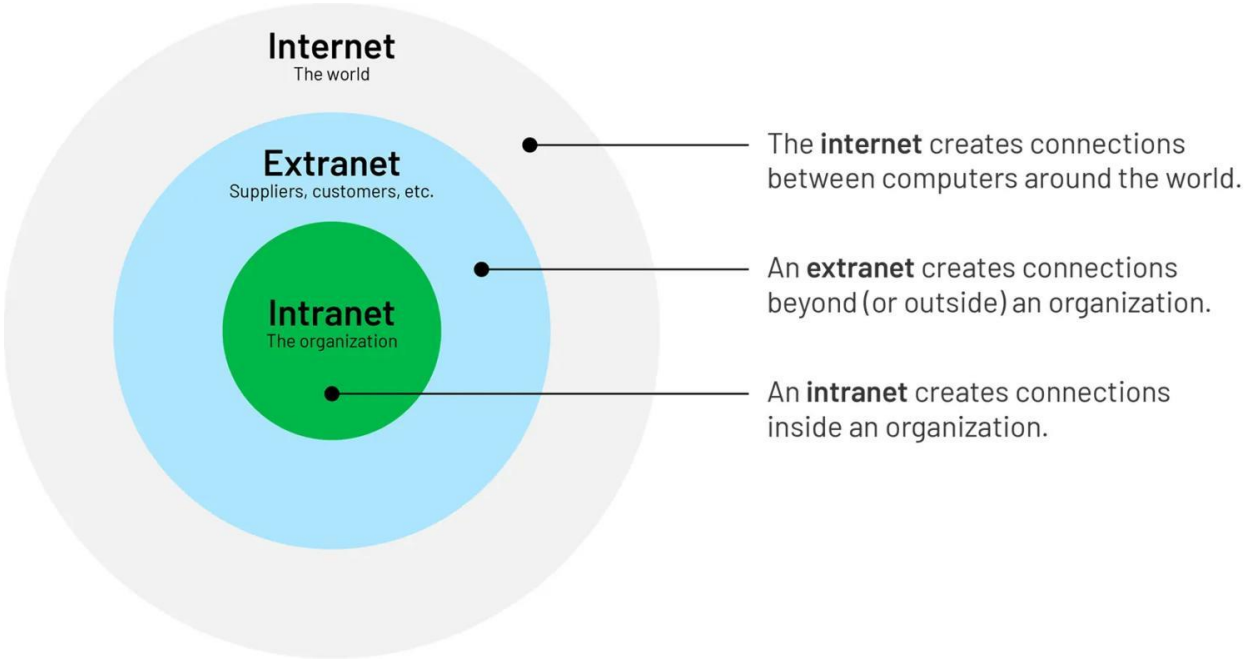


Пример. Производственная компания может предоставить поставщикам доступ к порталу заказов. Поставщик видит сведения о необходимых материалах и сроках поставки, но не получает доступа к бухгалтерским документам и кадровой информации.

2.4. Различия между интрасетью и экстрасетью

Критерий	Интрасеть	Экстрасеть
Назначение	Внутренняя работа организации	Взаимодействие с внешними участниками
Пользователи	Сотрудники организации	Сотрудники и авторизованные внешние пользователи
Доступ	Внутренний или удалённый защищённый	Ограниченный внешний доступ
Информация	Внутренние документы и данные	Данные, необходимые для совместной работы
Безопасность	Контроль доступа сотрудников	Дополнительное разграничение прав внешних пользователей

2.5. Связь Интернета, интрасети и экстрасети



Интернет, интрасеть и экстрасеть используют общие сетевые технологии, но отличаются назначением и правилами доступа.

- Интернет предоставляет глобальный доступ к общедоступным ресурсам.
- Интрасеть предназначена для внутренней работы организации.
- Экстрасеть обеспечивает ограниченный доступ внешних пользователей к отдельным корпоративным ресурсам.

Для защиты интрасети и экстрасети применяются межсетевые экраны, средства аутентификации, VPN и механизмы разграничения доступа.

3. Уязвимые места сетевой структуры с IP-протоколом

3.1. Общие сведения

IP (Internet Protocol) является основным протоколом сетевого уровня модели TCP/IP. Он обеспечивает адресацию устройств и передачу пакетов между различными сетями.

В корпоративных сетях IP применяется для обмена данными между компьютерами, серверами, маршрутизаторами и другими устройствами.

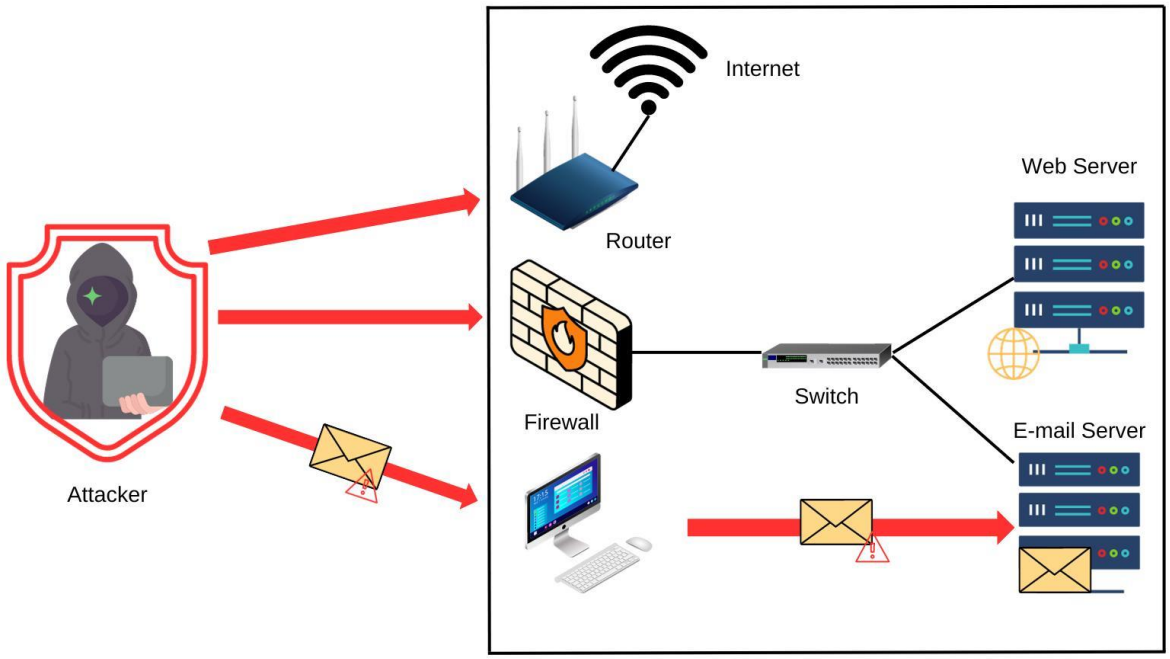
Однако использование IP не гарантирует безопасность передаваемой информации.

IP отвечает за доставку пакетов по сети, но сам по себе не обеспечивает:

- шифрование данных;
- проверку личности отправителя;
- конфиденциальность передаваемой информации;
- защиту от подмены адресов;
- предотвращение всех видов сетевых атак.

Поэтому в корпоративных сетях применяются дополнительные средства защиты.

3.2. Основные уязвимые места IP-сети



1. Уязвимости IP-адресации

IP-адрес используется для идентификации сетевого интерфейса. Однако сам по себе IP-адрес не подтверждает личность пользователя или устройства.

Злоумышленник может использовать подмену IP-адреса (IP Spoofing). При такой атаке в заголовке пакета указывается ложный адрес отправителя.

2. Уязвимости маршрутизаторов

Маршрутизаторы передают пакеты между сетями и определяют путь их движения.

К возможным проблемам относятся:

- слабые пароли для управления;
- устаревшее программное обеспечение;
- неправильные правила маршрутизации;
- открытые интерфейсы удалённого управления;
- отсутствие контроля доступа.

Если маршрутизатор будет скомпрометирован, злоумышленник может получить возможность перехвата или перенаправления сетевого трафика.

3. Уязвимости коммутаторов

Коммутаторы объединяют устройства внутри локальной сети. Ошибки в настройках могут привести к несанкционированному доступу к сетевым сегментам.

Примеры угроз:

- MAC Flooding;
- VLAN Hopping;
- подключение неизвестных устройств;

- использование незащищённых сетевых портов.

4. Уязвимости серверов

Серверы содержат важные корпоративные данные и предоставляют сетевые услуги.

Основные причины уязвимости:

- устаревшие версии программ;
- слабые пароли;
- отсутствие обновлений безопасности;
- избыточные права пользователей;
- неправильно настроенные службы.

5. Уязвимости каналов передачи данных

Если передача информации не защищена шифрованием, злоумышленник может попытаться перехватить сетевой трафик.

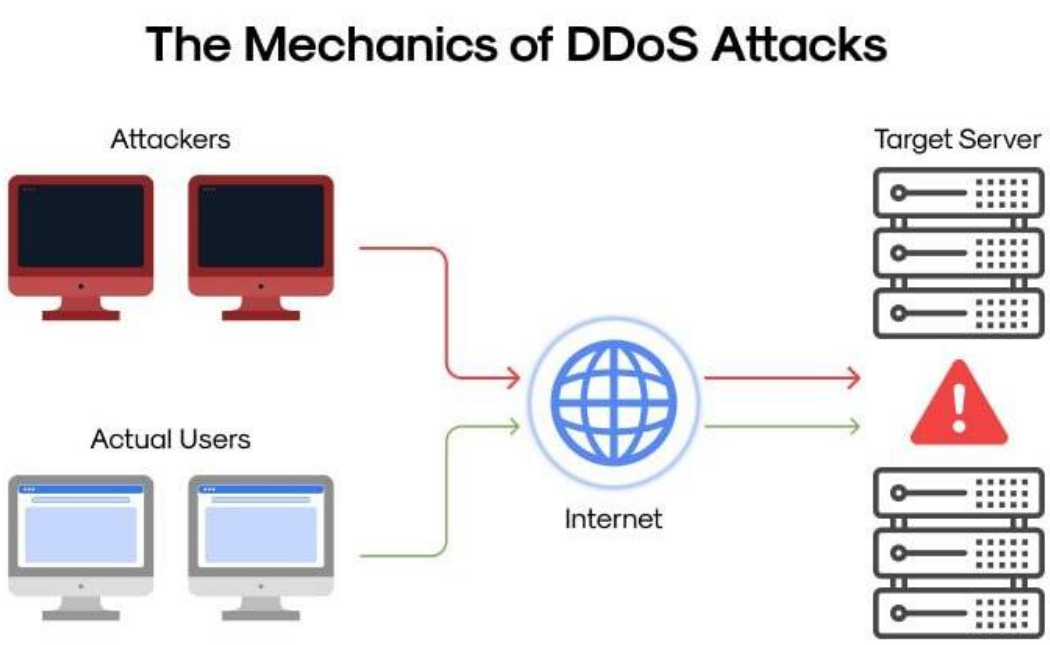
Примером является атака типа Man-in-the-Middle (MITM), при которой злоумышленник вмешивается в обмен данными между двумя сторонами.

3.3. Основные виды сетевых атак

Вид атаки	Сущность атаки	Возможные последствия
IP Spoofing	Подмена IP-адреса отправителя	Обход отдельных механизмов фильтрации
DoS	Перегрузка сетевого ресурса запросами	Нарушение доступности
DDoS	Распределённая атака на ресурс	Отказ в обслуживании
Man-in-the-Middle	Перехват или изменение данных между сторонами	Утечка и подмена информации
Port Scanning	Проверка открытых портов устройства	Обнаружение доступных служб
ARP Spoofing	Подмена ARP-сообщений в локальной сети	Перехват или перенаправление трафика
DNS Spoofing	Подмена DNS-ответов	Перенаправление на вредоносные ресурсы
Packet Sniffing	Перехват и анализ сетевых пакетов	Получение конфиденциальной информации

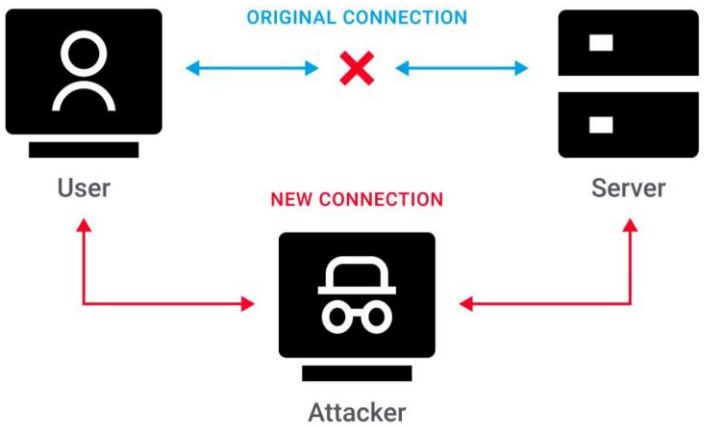
3.4. Примеры сетевых угроз

Пример 1. Атака DoS



Злоумышленник отправляет большое количество запросов на сервер. Ресурсы сервера расходуются на обработку этих запросов. В результате обычные пользователи могут потерять доступ к сервису.

Пример 2. Атака Man-in-the-Middle



Злоумышленник размещается между двумя участниками обмена данными. Он может перехватывать или изменять информацию, если передача не защищена должным образом.

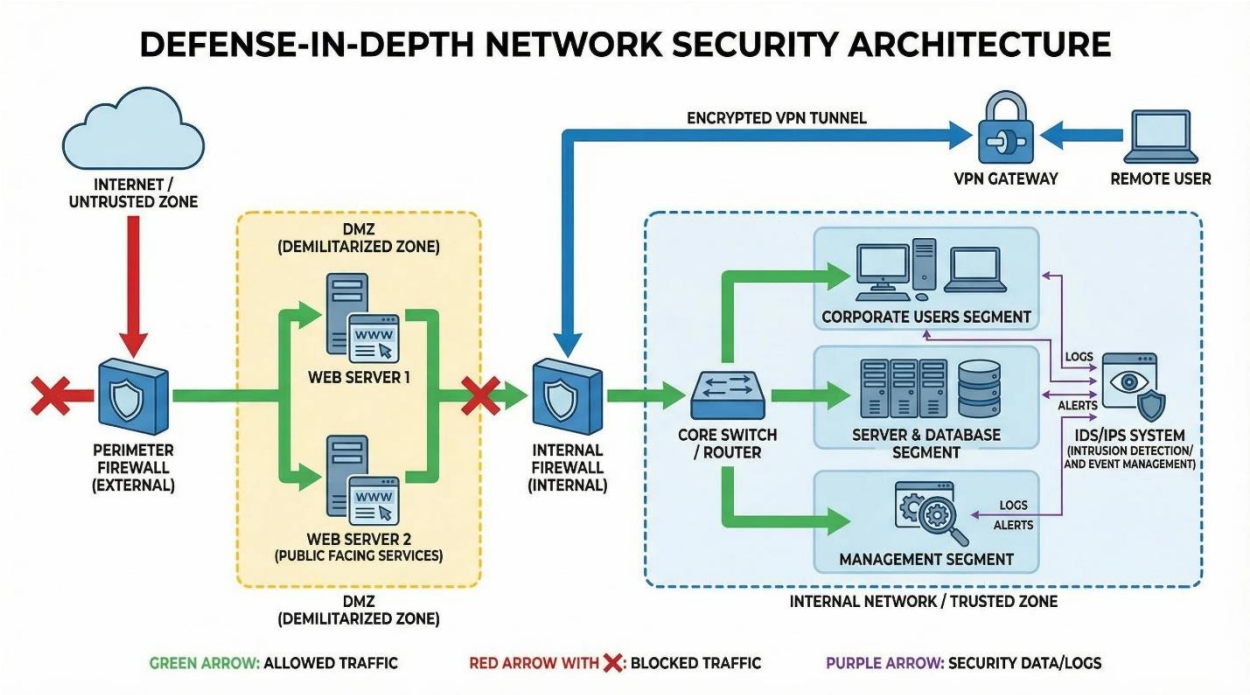
Пример 3. Подмена IP-адреса

Злоумышленник формирует IP-пакет с поддельным адресом отправителя. Если система проверки не выявляет такую подмену, пакет может быть принят как часть разрешённого обмена.

3.5. Методы защиты корпоративной IP-сети

Для снижения рисков применяются технические и организационные меры.

Средство защиты	Назначение
Firewall	Фильтрация входящего и исходящего трафика
VPN	Защищённая передача данных через общедоступные сети
IDS	Обнаружение подозрительной сетевой активности
IPS	Обнаружение и блокирование сетевых атак
VLAN	Разделение сети на логические сегменты
ACL	Ограничение доступа на основе правил
Шифрование TLS/IPsec	Защита передаваемой информации
MFA	Многофакторная проверка пользователей
Антивирусная защита	Обнаружение вредоносных программ
Резервное копирование	Восстановление данных после сбоев и атак



3.6. Сегментация корпоративной сети

Одним из важных методов защиты является разделение корпоративной сети на отдельные сегменты.

Например, в университете могут быть созданы следующие VLAN:

VLAN	Назначение
VLAN 10	Администрация
VLAN 20	Преподаватели
VLAN 30	Студенты
VLAN 40	Серверы
VLAN 50	Гостевой Wi-Fi

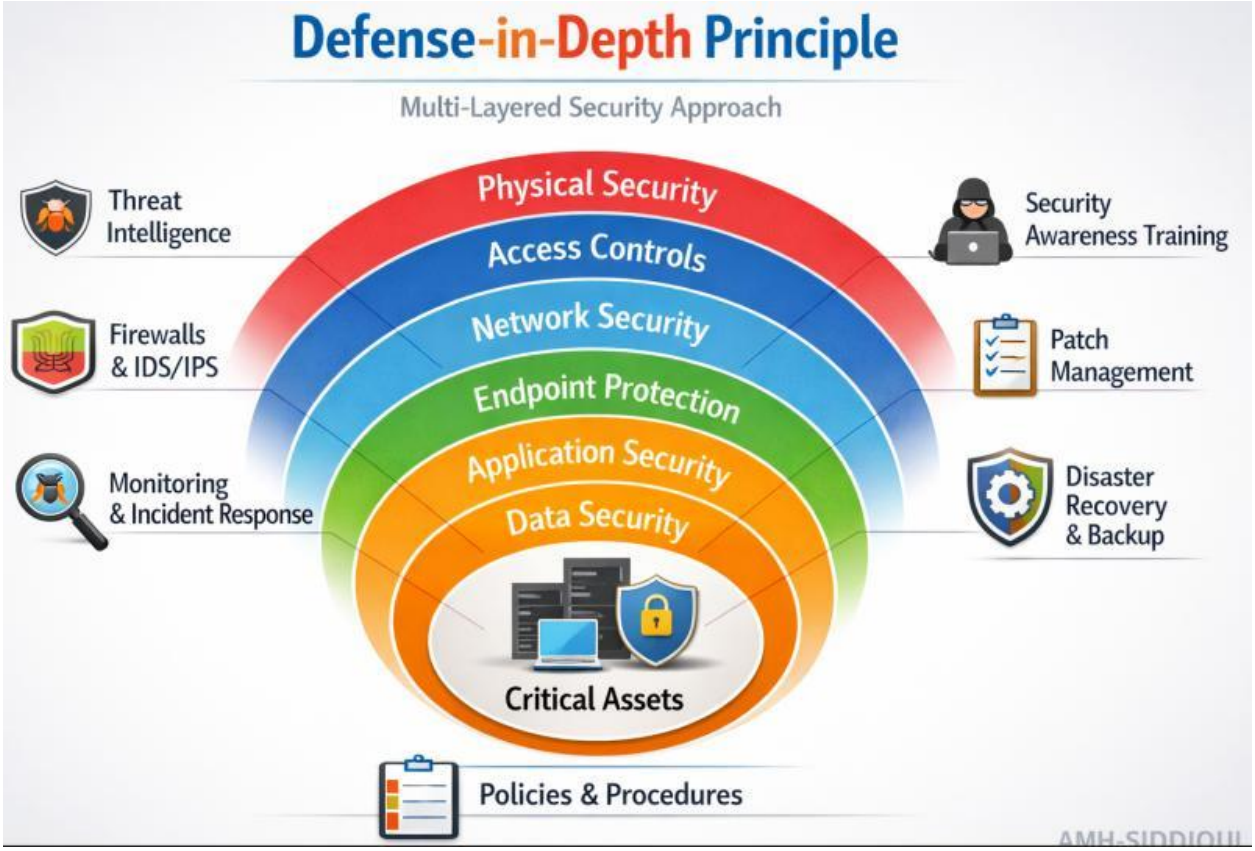
Такое разделение позволяет ограничить прямой обмен данными между различными группами пользователей.

Например, студенты могут получать доступ к учебным серверам, но не должны иметь прямого доступа к компьютерам бухгалтерии.

Для взаимодействия между VLAN применяются маршрутизация и списки контроля доступа ACL.

3.7. Принцип многоуровневой защиты

Защита корпоративной сети не должна зависеть только от одного устройства или программы. Для этого используется несколько уровней безопасности.



Основные уровни защиты:

1. Физический уровень. Ограничение доступа к серверным помещениям и сетевому оборудованию.
2. Сетевой уровень. Использование маршрутизаторов, firewall, VLAN и ACL.
3. Транспортный уровень. Применение защищённых соединений и шифрования.
4. Прикладной уровень. Проверка пользователей и защита веб-приложений.
5. Уровень данных. Контроль доступа к файлам, базам данных и резервным копиям.

Если один уровень защиты не обнаружит угрозу, другие уровни могут ограничить её последствия.

4. Практические примеры применения корпоративных сетей

Пример 1. Корпоративная сеть университета

В университете создаётся единая сеть для учебных корпусов. В ней объединяются:

- административные компьютеры;

- компьютерные классы;
- серверы электронного обучения;
- библиотечные ресурсы;
- беспроводные точки доступа.

Для студентов создаётся отдельный сегмент. Доступ к административным ресурсам ограничивается.

Пример 2. Корпоративная сеть предприятия

Предприятие имеет главный офис и несколько филиалов. Все подразделения подключаются через защищённые VPN-каналы.

Сотрудники филиалов получают доступ к общей базе данных, системе управления заказами и корпоративной почте.

Пример 3. Экстрасеть для поставщиков

Предприятие предоставляет поставщикам доступ к отдельному веб-порталу. Через него можно просматривать заказы и отправлять сведения о поставках. Доступ к внутренним финансовым документам запрещён.

5. Контрольные вопросы

1. Что такое корпоративная сеть?
2. Какие основные компоненты входят в её состав?
3. Какие задачи выполняет уровень доступа?
4. Для чего предназначена интрасеть?
5. Что такое экстрасеть?
6. Чем интрасеть отличается от экстрасети?
7. Какую роль выполняет протокол IP?
8. Почему IP сам по себе не обеспечивает безопасность данных?
9. Что такое IP Spoofing?
10. В чём заключается атака Man-in-the-Middle?
11. Для чего применяется межсетевой экран?
12. Какую задачу выполняет VLAN?
13. Чем IDS отличается от IPS?
14. Почему корпоративную сеть необходимо разделять на сегменты?

6. Практические задания

Задание 1. Проектирование корпоративной сети

Представьте, что необходимо создать сеть для университета, в котором имеются:

- административный отдел;
- кафедры;
- компьютерные классы;
- библиотека;
- серверная комната.

Составьте схему сети и определите:

1. Какие устройства необходимы?
2. Какие отделы следует объединить в отдельные VLAN?
3. Где необходимо разместить маршрутизатор и межсетевой экран?
4. Какие ресурсы должны быть доступны студентам?
5. Какие ресурсы должны быть доступны только администрации?

Задание 2. Сравнение интрасети и экстрасети

Приведите по три примера использования интрасети и экстрасети в университете или на предприятии.

Задание 3. Анализ сетевых угроз

Рассмотрите следующие ситуации и определите возможную угрозу и способ защиты:

Ситуация	Вопрос
Неизвестный компьютер подключён к сети организации	Как ограничить доступ?
Сервер перестал отвечать из-за большого количества запросов	Какая атака могла быть выполнена?
Сотрудник использует открытый Wi-Fi для передачи документов	Какие риски существуют?
Студент получил доступ к административному серверу	Какие ошибки могли быть допущены?

7. Заключение

Корпоративные сети обеспечивают взаимодействие сотрудников, подразделений и внешних партнёров организации. Внутренние ресурсы предоставляются через интрасеть, а ограниченный доступ внешним участникам обеспечивается посредством экстрасети.

Протокол IP служит основой передачи данных между сетями, но не гарантирует их полную защиту. Поэтому для безопасной работы корпоративной сети необходимо применять межсетевые экраны, VPN, VLAN, ACL, IDS/IPS и средства шифрования.

Главный вывод: надёжность корпоративной сети зависит не только от скорости передачи данных, но и от правильной архитектуры, разграничения доступа и защиты информации.