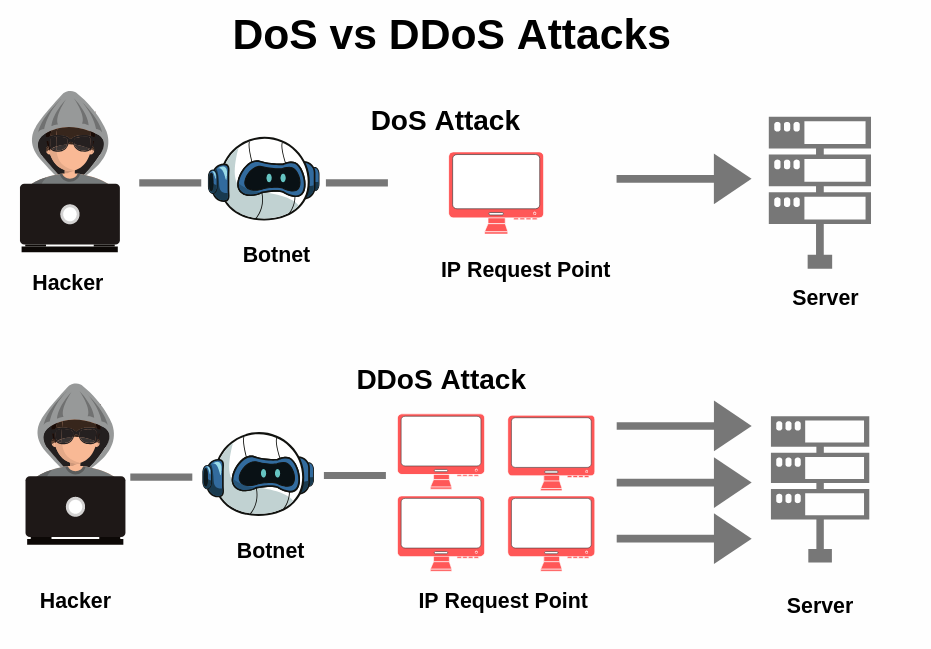
Сетевые атаки

# **DoS/DDoS-атаки**

**DoS- и DDoS-атаки** — это формы кибератак, направленные на нарушение работы интернет-сервисов. Однако они отличаются масштабом и способом выполнения.



## DoS-атака

**DoS (Denial of Service)** — атака, цель которой — сделать сайт или ресурс недоступным для пользователей. Это достигается путём отправки большого количества запросов на сервер, что перегружает систему и приводит к отказу в обслуживании.

Особенности:

* Обычно осуществляется с одного компьютера или виртуальной машины.
* Атакующий использует специальные программы для создания интенсивного трафика.

## DDoS-атака

**DDoS (Distributed Denial of Service) —** распределённая атака, при которой множество устройств (например, компьютеров или IoT-устройств) одновременно отправляют запросы на сервер. Это создаёт нагрузку, превышающую возможности системы, и делает ресурс недоступным.

Особенности:

* Трафик направляется на сервер с разных IP-адресов, что затрудняет блокировку.
* Злоумышленники создают ботнеты — сети заражённых устройств, которые управляются удалённо.

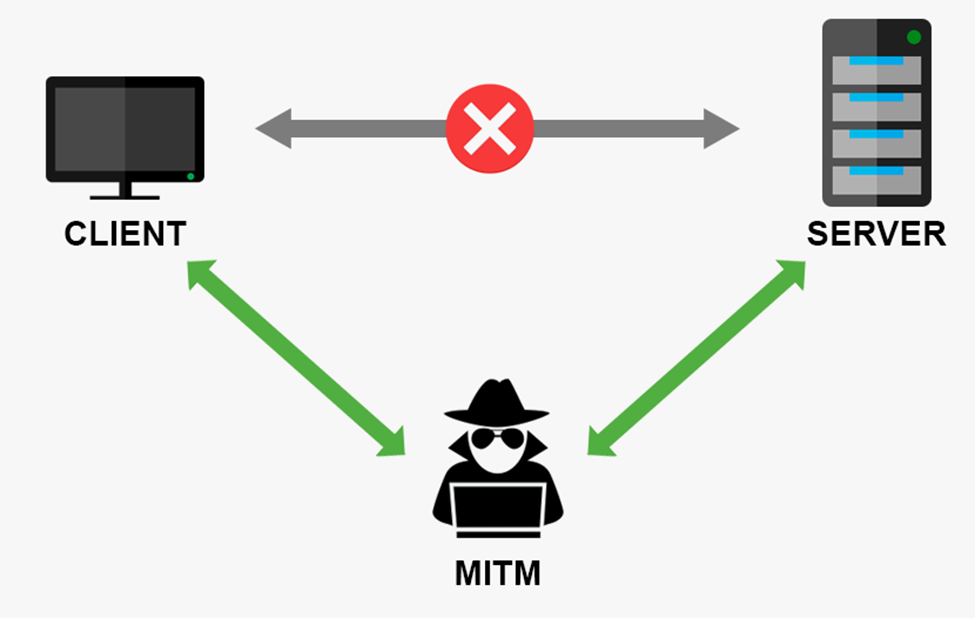
## Методы защиты

Для защиты от DoS- и DDoS-атак используются, например:

* Фильтрация трафика — специализированные системы анализируют входящий трафик и блокируют подозрительные запросы.
* Ограничение пропускной способности — установка лимитов на объём передаваемых данных позволяет избежать перегрузки сети.
* Использование прокси-серверов и балансировщиков нагрузки — эти инструменты помогают перераспределить запросы, снижая нагрузку на основные узлы системы.
* Мониторинг и анализ трафика — постоянный контроль сетевой активности позволяет оперативно реагировать на потенциальные угрозы.

# “Человек посередине”

**MITM (Man-in-the-Middle, «человек посередине»)** — это тип кибератаки, при которой злоумышленник «пропускает» веб-трафик жертвы «через себя». Он может подслушивать, читать переписку либо притворяться участником разговора.



**Перехват трафика** — первый этап MITM-атаки. Злоумышленник вмешивается в процесс передачи данных из/в сеть жертвы, перехватывая их с помощью «подставной» сети прежде, чем они будут реально отправлены адресату или поступят в сеть жертвы.

Некоторые способы перехвата трафика:

1. **Пассивная атака**. Злоумышленник создаёт Wi-Fi-точки со свободным доступом (без пароля и авторизации). Когда пользователь подключается к такой точке, атакующий получает доступ ко всему трафику, проходящему через неё, и может выделить из него любые данные для перехвата.
2. **Активный перехват**. Может быть осуществлён несколькими вариантами:

* **IP-spoofing** — подмена IP-адреса цели в заголовке пакета на адрес атакующего. В результате пользователи, вместо того чтобы зайти на запрашиваемый URL, попадают на сайт злоумышленника.
* **ARP-spoofing** — подмена настоящего MAC-адреса узла на адрес атакующего в ARP-таблице жертвы. В результате данные, отправленные пользователем на IP-адрес требуемого узла, попадают на адрес атакующего.
* **DNS-spoofing** — заражение кэша DNS, проникновение на сервер DNS и подмена записи соответствия адреса веб-сайта.
* **SSL-stripping** — понижение соединения с защищённого HTTPS до простого HTTP, перехват TLS-аутентификации, отправленной приложением пользователю.

Подмена трафика может происходить, например, когда злоумышленник изменяет банковские данные во время онлайн-транзакции, перенаправив средства на свой счёт.

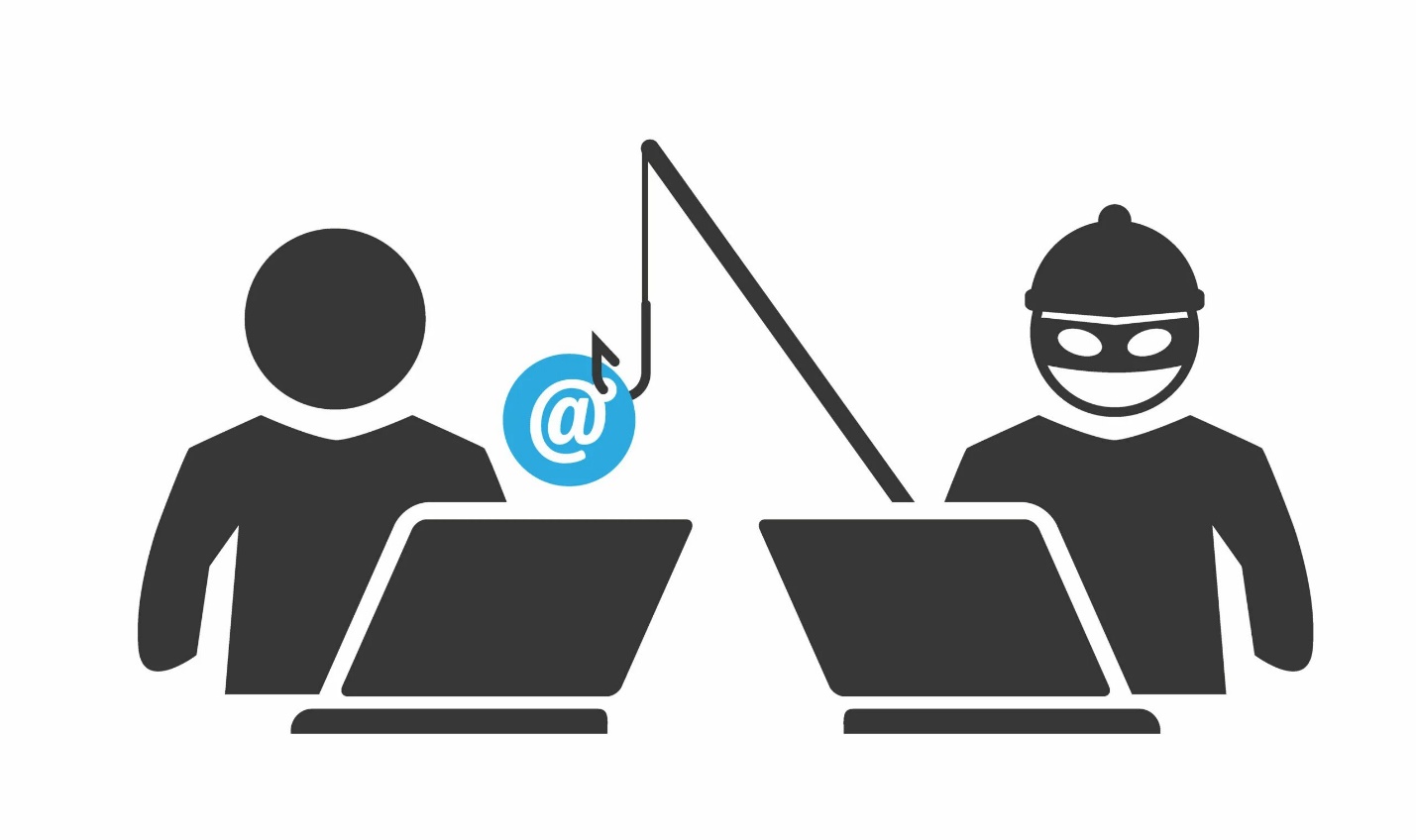
## Методы защиты

Как и от других атак существуют методы защиты от MITM. Полная защита от MITM-атак невозможна, но можно значительно снизить риск следующими действиями:

* **Использование HTTPS**. Протокол SSL/TLS шифрует данные, передаваемые между веб-браузером и веб-сервером. Это делает перехват и чтение данных значительно сложнее.
* **Проверка сертификатов SSL/TLS**. Нужно убедиться, что сертификат веб-сайта действителен и выдан доверенным центром сертификации.
* **Двухфакторная аутентификация (2FA**). 2FA добавляет дополнительный уровень безопасности, требуя второго фактора аутентификации, например, кода из SMS-сообщения или приложения для аутентификации.
* **Проверка целостности пакетов**. Некоторые протоколы используют механизмы проверки целостности пакетов, которые позволяют обнаружить изменения данных во время передачи.
* **Обучение сотрудников**. Обучение сотрудников о рисках MITM-атак и методах защиты является важным аспектом обеспечения безопасности.

# Фишинг и социальная инженерия

**Фишинг** — это вид интернет-мошенничества, цель которого — получение доступа к конфиденциальным данным пользователей, в частности логинам и паролям. Злоумышленники отправляют поддельные электронные письма или сообщения, которые выглядят как официальные запросы от банков, компаний или госучреждений.



## Методы фишинга:

* **Фейковые предупреждения безопасности**. Например, сообщение от «службы безопасности» игры с предупреждением о якобы взломе аккаунта и просьбой перейти по ссылке для «восстановления доступа».
* **Сообщения о выигрыше или бонусах**. Пользователей соблазняют «бесплатными» наградами, премиум-валютой или редкими предметами.
* **Использование обмана в PvP-играх**. Мошенники могут создавать фальшивые аккаунты игроков, выдавая себя за друзей или гильдмастеров, чтобы выманить конфиденциальную информацию.

**Социальная инженерия** — это способы обмана, манипуляции и введения в заблуждение. Злоумышленники используют человеческие слабости, такие как доверие, страх, спешку, неуверенность или жажду помощи, чтобы получить доступ к конфиденциальной информации, ресурсам или системам.

Некоторые методы социальной инженерии:

* **Вишинг**. Фейковые звонки, во время которых злоумышленники представляются сотрудниками банков, правоохранительных органов или других организаций и убеждают жертв предоставить им личные данные или совершить финансовые операции.
* **Смишинг**. Мошенничество через SMS-сообщения, в которых содержится ссылка на «официальный» сайт банка, доставки или налоговой службы.
* **«Предлог».** Метод основан на создании убедительной легенды, когда злоумышленник представляет себя сотрудником компании, доставщика, представителем службы безопасности.

# Атаки на пароли

Одной из самой распространенных атак такого вида считается брутфорс.

**Брутфорс (brute force), или атака полным перебором**, — это метод взлома, при котором хакер подбирает разные варианты логинов, паролей и ключей шифрования. Цель — войти в систему или получить доступ к защищённым данным.



**Суть брутфорса** — перебор всех возможных комбинаций. Злоумышленник начинает с самой простой комбинации и постепенно увеличивает сложность, пока не найдёт правильный пароль или ключ.

Виды брутфорс-атак:

* **Классический**. Полный перебор всех возможных комбинаций символов без учёта контекста. Короткие и слабые пароли такой метод способен подобрать легко, более сложные — гораздо сложнее.
* **Словарная атака**. Злоумышленник использует готовый список паролей вместо полного перебора. Такой метод хоть и работает статистически быстрее классического, но неэффективен против уникальных паролей.
* **Гибридный брутфорс**. Использует пароли из словаря и добавляет к ним цифры, спецсимволы, заглавные буквы.
* **Обратная атака**. Если при брутфорсе к одному логину подбирают множество вариантов паролей, то при обратной атаке один пароль подставляют к разным логинам.

## Методы защиты:

Для защиты от брутфорс-атак рекомендуется использовать комплексный подход, так как одного метода недостаточно, так как злоумышленники могут применять разные способы взлома. Для комплексного подхода можно применить такие методы, как:

* **Создание сложных паролей**. Для каждой учётной записи нужно использовать уникальные комбинации. Пароль должен быть достаточно длинным и включать прописные и заглавные буквы, цифры, специальные символы.
* **Двухфакторная аутентификация (2FA**). Даже если пароль будет скомпрометирован, злоумышленнику потребуется доступ к телефону для подтверждения входа.
* **Использование биометрии**. По возможности можно применять биометрическую аутентификацию, такую как отпечаток пальца или распознавание лица.
* **Ограничение количества авторизаций**. После нескольких безуспешных попыток необходимо блокировать возможность дальнейших действий.
* **Мониторинг и логирование**. Позволяет вовремя выявить подозрительные попытки входа. Анализ логов помогает быстро обнаружить атаки и принять меры по их предотвращению.
* **Шифрование данных и базы**. Даже если мошенники взломают учётную запись, они не смогут прочитать информацию без ключа дешифровки.