



Основы построения защищенных компьютерных сетей

Лекция 13
Виртуальные частные сети

Семён Новосёлов

2025

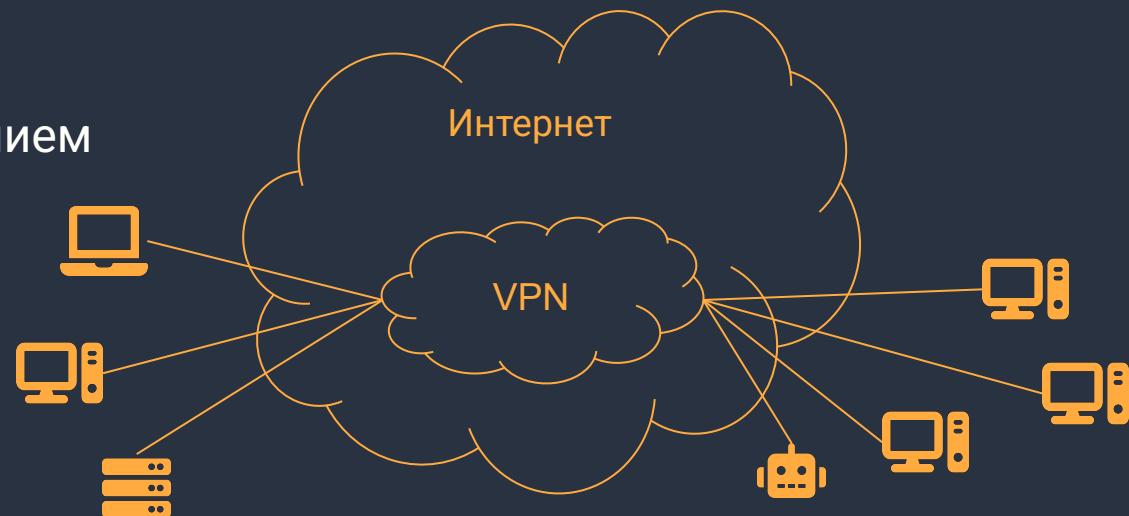


БОУ
имени И. Канта

Виртуальная частная сеть (VPN)

Технология, позволяющая развернуть закрытую частную сеть поверх другой открытой сети.

- чаще всего с использованием шифрования



Для чего используется VPN?

организациями – для связи в единую сеть своих подразделений из различных локаций

интернет-провайдерами – для подключения клиентов

- например, в связке из Ethernet-сети и VPN-сервера для контроля доступа

хакерами/преступниками – как часть мер по сокрытию следов атак и своей личности

пользователями

- для защиты при подключении к публичным сетям
 - например, при подключении к публичной сети Wi-Fi
- для безопасного удалённого доступа к своей сети
 - VPN-сервер на роутере + белый IP
- для обхода законодательных ограничений
 - например, блокировок сайтов с пиратским контентом

Принципы построения

VPN строится используя технологию **туннелирования** методом вкладывания пакетов (**инкапсуляции**) в данные протоколов TCP/IP.

Для обеспечения безопасности используется:

- **шифрование** – для предотвращения перехвата данных
- **аутентификация** – для проверки подлинности пользователей
- **коды аутентификации сообщений (MAC)** – для проверки целостности пакетов

Частные сети без шифрования

- Полезны для обхода физических ограничений
 - организация нескольких изолированных сетей поверх одной физической
- Используются провайдерами для подключения клиентов к сети Интернет
- Пример протокола – L2TP
- Могут использоваться в связке с другими технологиями VPN на высоких уровнях модели OSI для обеспечения функций защиты данных – шифрования, аутентификации, проверки подлинности сообщений

Типы VPN

1. Хост-Сеть

- для подключения отдельных компьютеров к сети
- может использоваться для подключения удаленных работников
- безопасный удалённый доступ к своей сети

2. Сеть-Сеть

- объединение нескольких сетей в одну виртуальную
- может использоваться для соединения подразделений организации

VPN на разных уровнях OSI

Канальный уровень (Layer 2)

L2TP

Сетевой уровень (Layer 3)

IPSec

- как правило представляется функция разграничения сетей
- функция защиты данных осуществляется протоколом на следующем уровне

- надстройка над протоколом IP
- обеспечивает функции защиты данных

VPN на транспортном уровне

Протоколы VPN могут также работать за счёт организации туннелей поверх транспортных протоколов (TCP, UDP)

Пример: **OpenVPN**

Недостатки:

- скорость работы меньше, а использование трафика больше, чем у IPSec

Достоинства:

- проще в настройке
- универсальней



- система с открытым исходным кодом
- использует протокол на основе SSL/TLS и библиотеки OpenSSL
- VPN строится поверх TCP/UDP
- поддерживаются все основные платформы:
Windows, Linux, Android, iOS

openvpn.net



WireGuard

- система с открытым исходным кодом
- встроен в ядро Linux
- значительно проще в настройке, чем OpenVPN
- VPN строится поверх UDP
- обfuscation, работа поверх TCP – отдаётся на верхний уровень
- поддерживаются все основные платформы:
Windows, Linux, Android, iOS

www.wireguard.com

VPN как средство обеспечения анонимности

- VPN позволяет скрыть свой IP-адрес Интернет-провайдера на IP-адрес VPN-провайдера
- при этом VPN-провайдер имеет полный доступ к сетевому трафику
- трекеры на сайтах и техники “device fingerprinting” работают при любом IP-адресе

Литература и ссылки

- Таненбаум Э., Уэзеролл Д. - Компьютерные сети. 5-е изд (2012)
- Инструкция по настройке OpenVPN-сервера:
<https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-ubuntu-20-04>