

Математические основы информационной безопасности

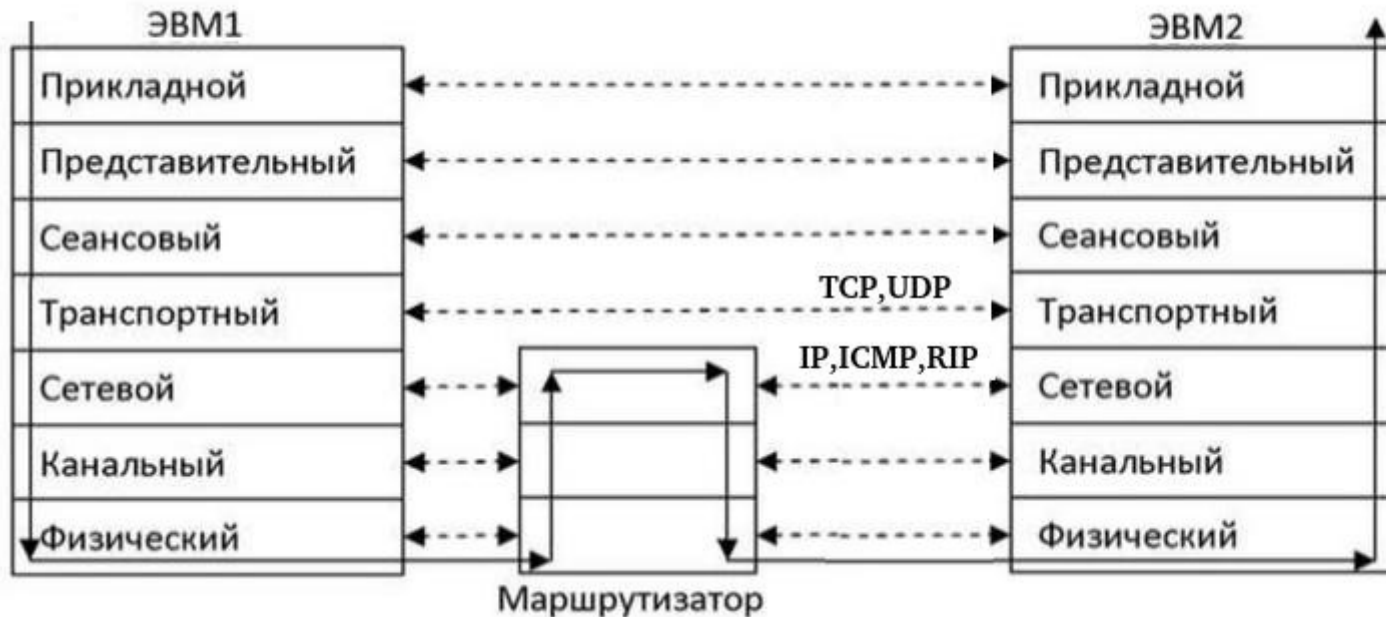
Груздев Дмитрий Николаевич

Защита данных в сети

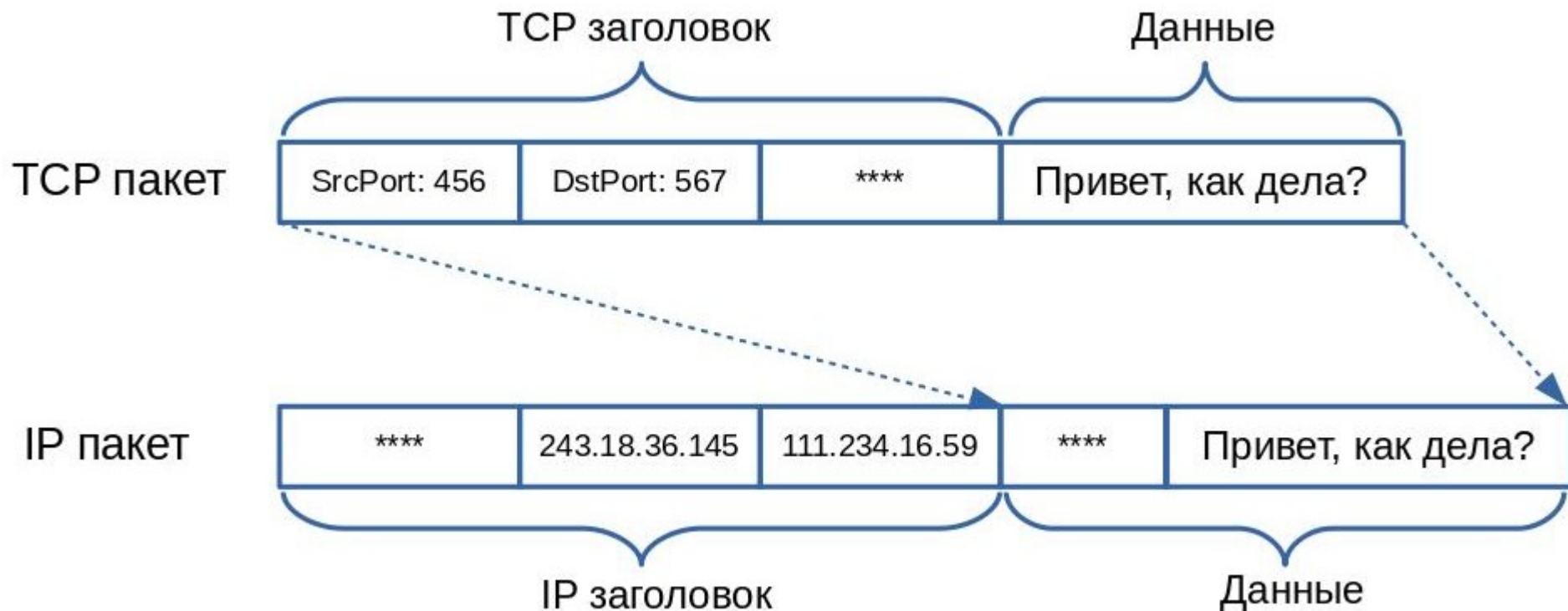
Модель ISO/OSI

ISO – International Standards Organization

OSI – Open Systems Interconnection

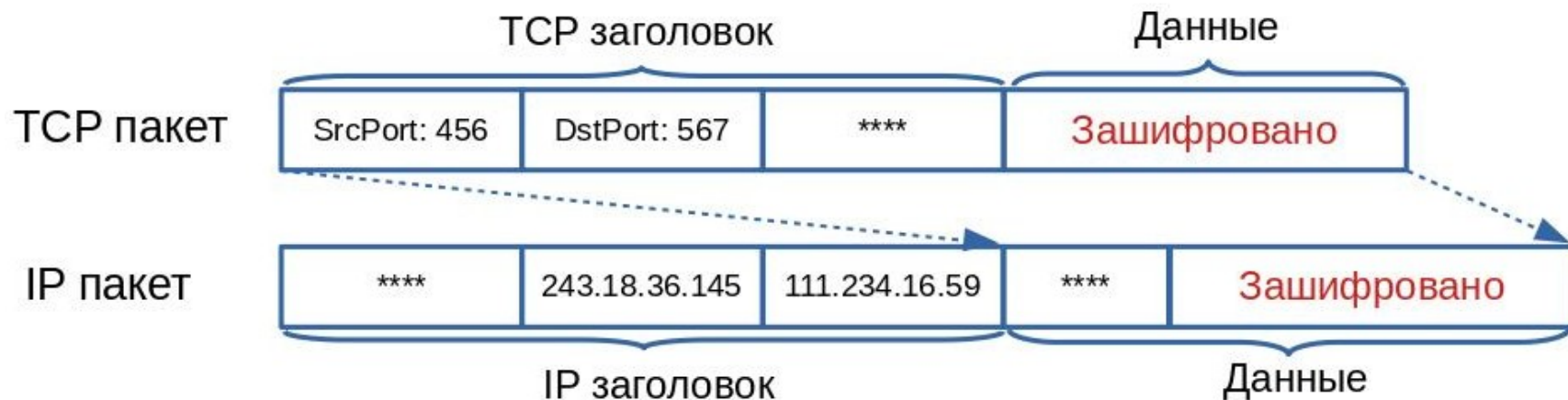


Сетевые пакеты

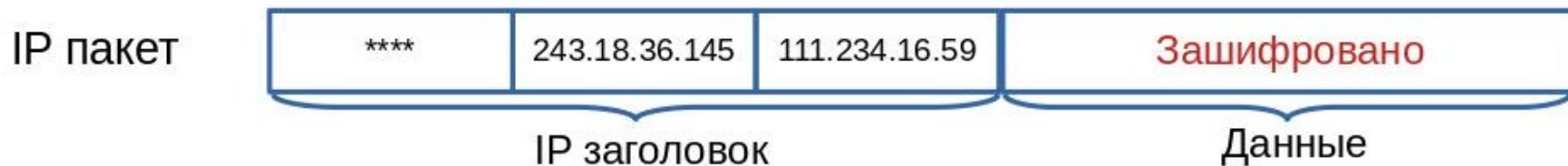


Зашифрованное соединение

Шифрование на TCP уровне

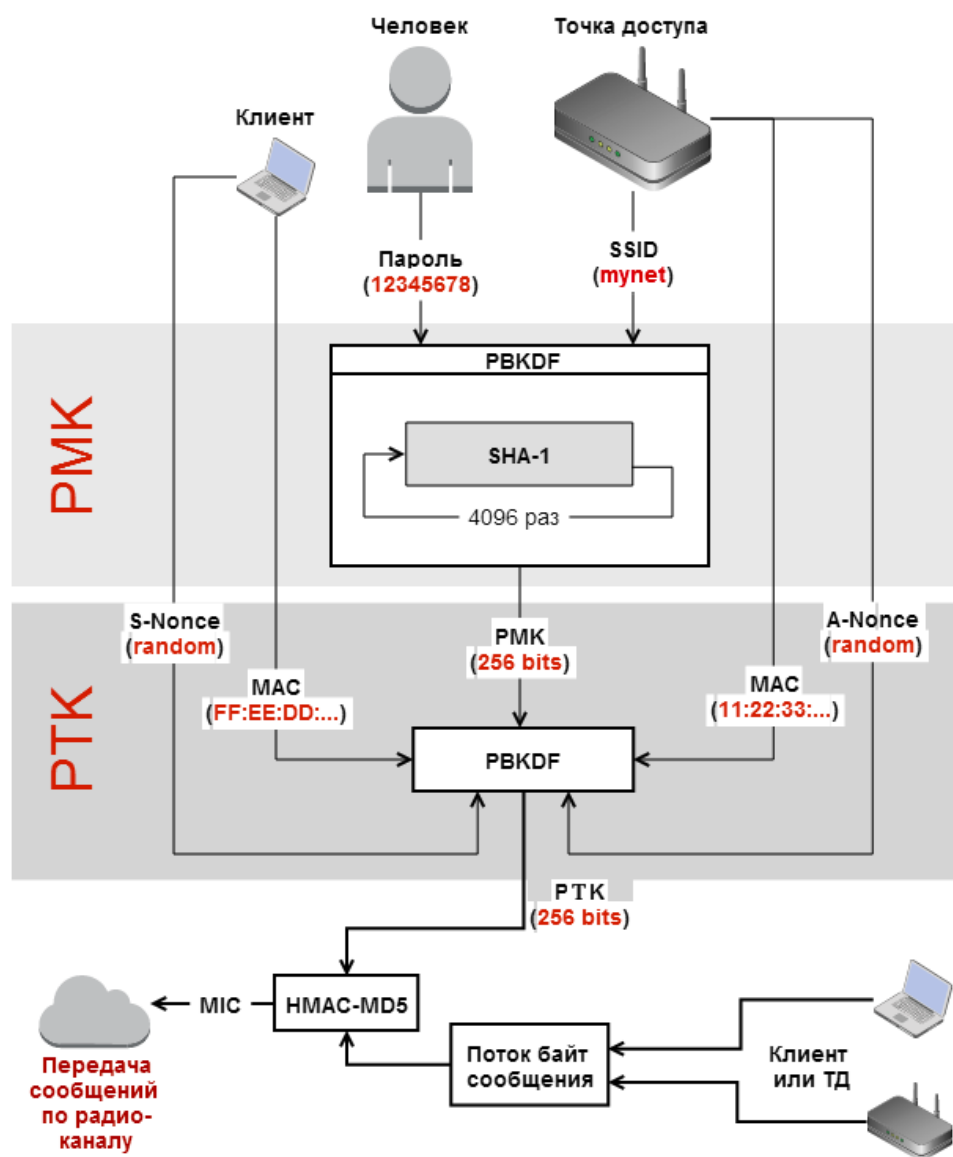


Шифрование на IP уровне



WPA handshake

- A-Nonce – случайное значение от станции
- S-Nonce – случайное значение от клиента
- PMK – главный парный ключ
- PTK – сеансовый ключ
- PBKDF - Password-Based Key Derivation Function



TLS handshake



Client

v 1.2



Server

- версия протокола
- поддерживаемые алгоритмы шифрования



- версия протокола
- алгоритм шифрования
- сертификат
- алгоритм выработки ключа сессии
- параметры для выработки ключа сессии



- параметры для выработки ключа сессии



- подтверждение



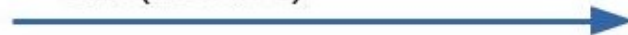
Client

v 1.3



Server

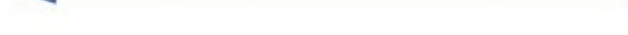
- версия протокола
- поддерживаемые алгоритмы шифрования
- параметры для выработки ключа сессии
- соль (32 байта)



- версия протокола
- алгоритм шифрования
- алгоритм выработки ключа сессии
- параметры для выработки ключа сессии
- соль (32 байта)

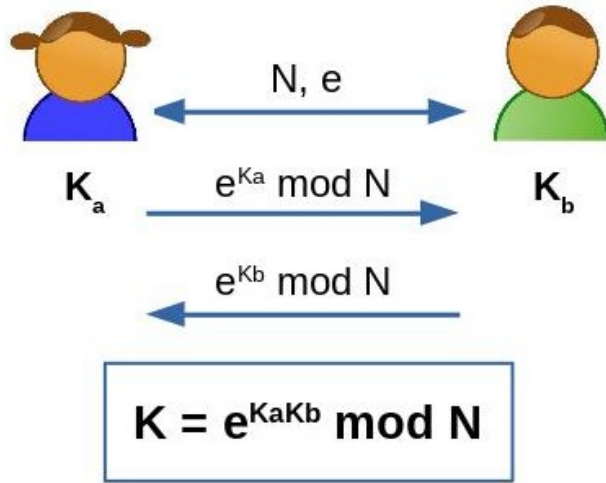
- сертификат

- подписанный handshake

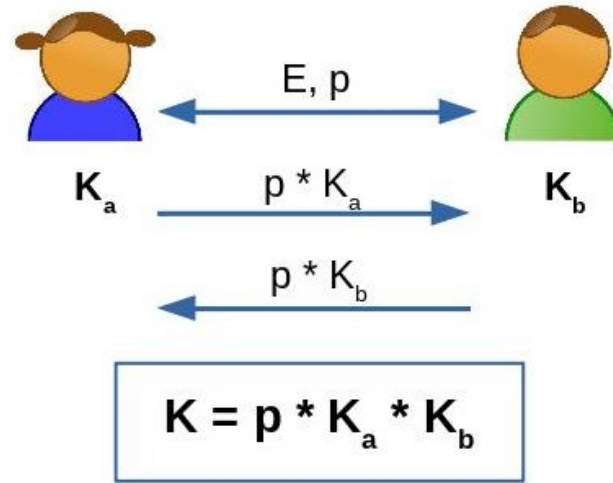


Выработка ключа шифрования

Алгоритм Диффи-Хелмана



Алгоритм Диффи-Хелмана на эллиптических кривых (ECDH)



Стандартизованные эллиптические кривые:

- X25519: $y^2 = x^3 + 486662x^2 + x$, $p = 9$ над $2^{255}-19$ – кривая Монтгомери
- secp192k1, secp192r1, secp224k1, secp224r1, secp384k1, secp384r1, secp521k1, secp521r1

Сертификаты

Поля сертификта:

Версия

Серийный номер

Алгоритм подписи

Имя издателя

Период действия

Имя субъекта

Открытый ключ

субъекта

ID издателя

ID субъекта

Расширения

Подпись



Сертификат безопасности сайта не является доверенным!

Вы попытались открыть [redacted], однако представленный сервером сертификат не является доверенным для операционной системы вашего ПК. Это может означать, что данный сервер сгенерировал собственные данные подтверждения безопасности, на которые Google Chrome не может полагаться, либо злоумышленник пытается перехватить данные коммуникации. Мы не советуем продолжать, **особенно** если вы не видели предупреждения для этого сайта ранее.

[Продолжить все равно](#)

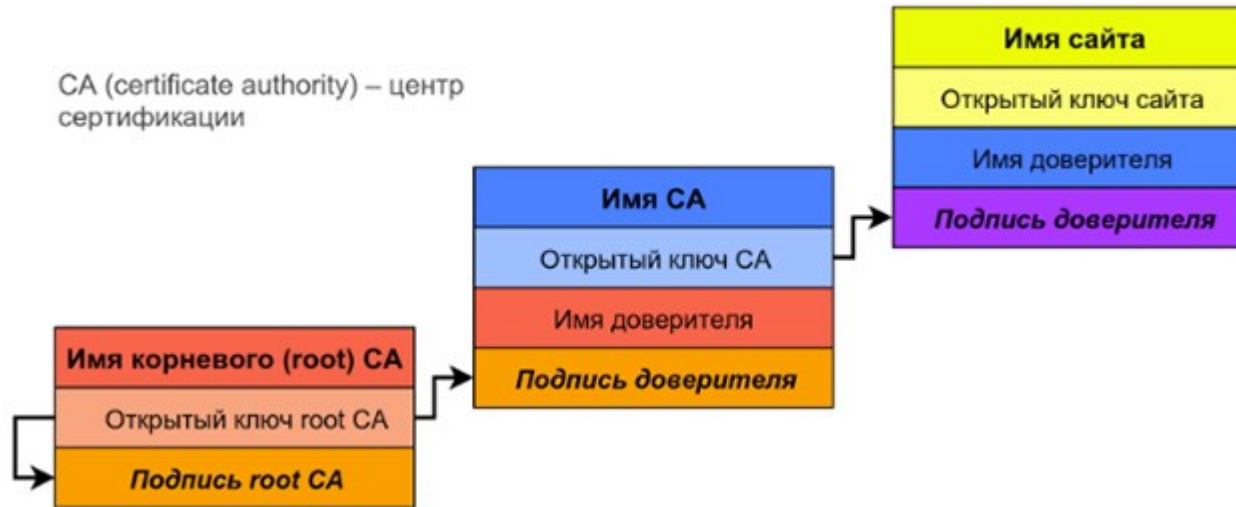
[Назад к безопасности](#)

► [Подробные сведения](#)

Угрозы при использовании недоверенных сертификатов:

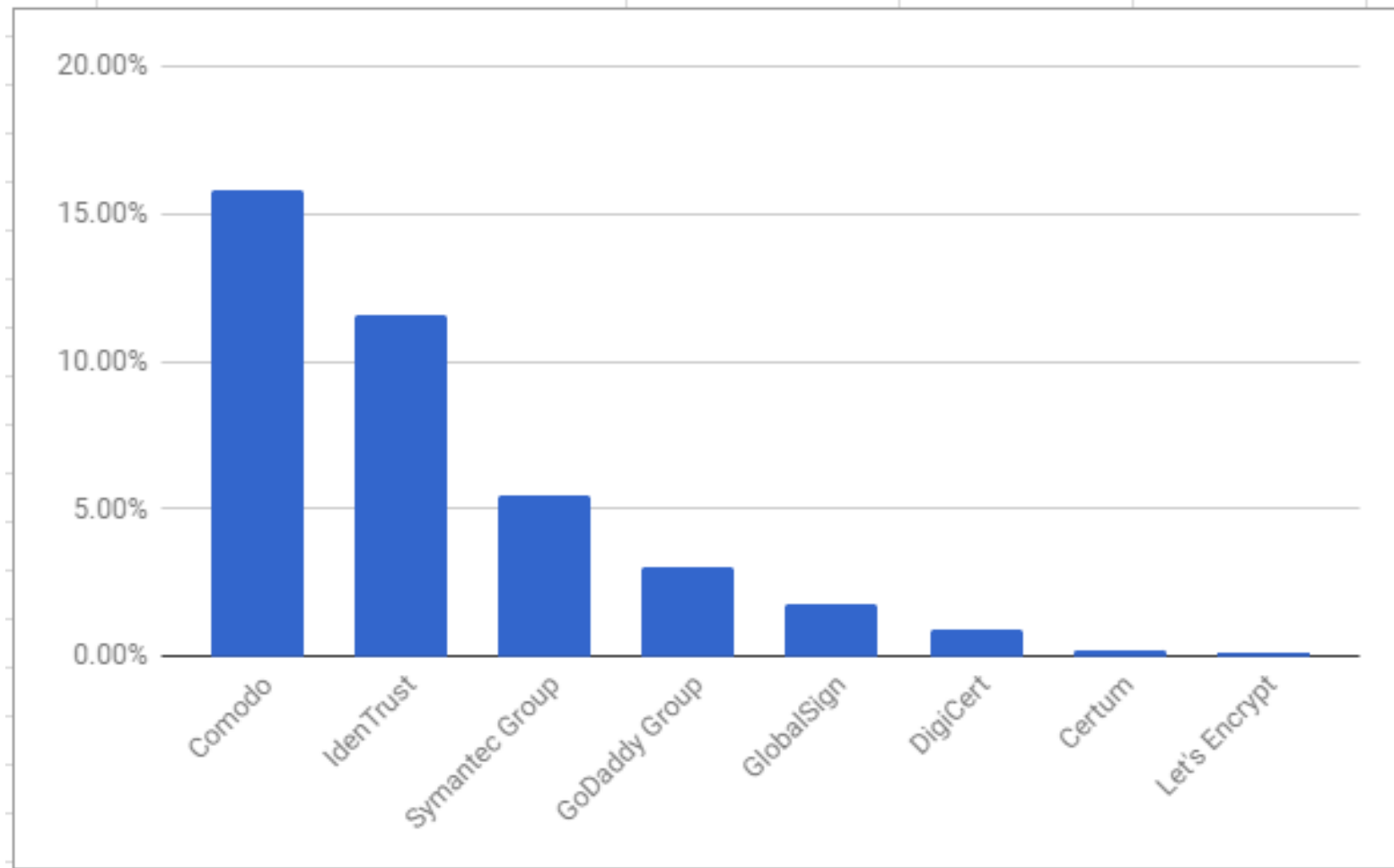
- Атака “человек посередине”
- Кража конфиденциальных данных

Цепочка сертификатов



Браузеры хранят корневые СА сертификаты.

Центры сертификации

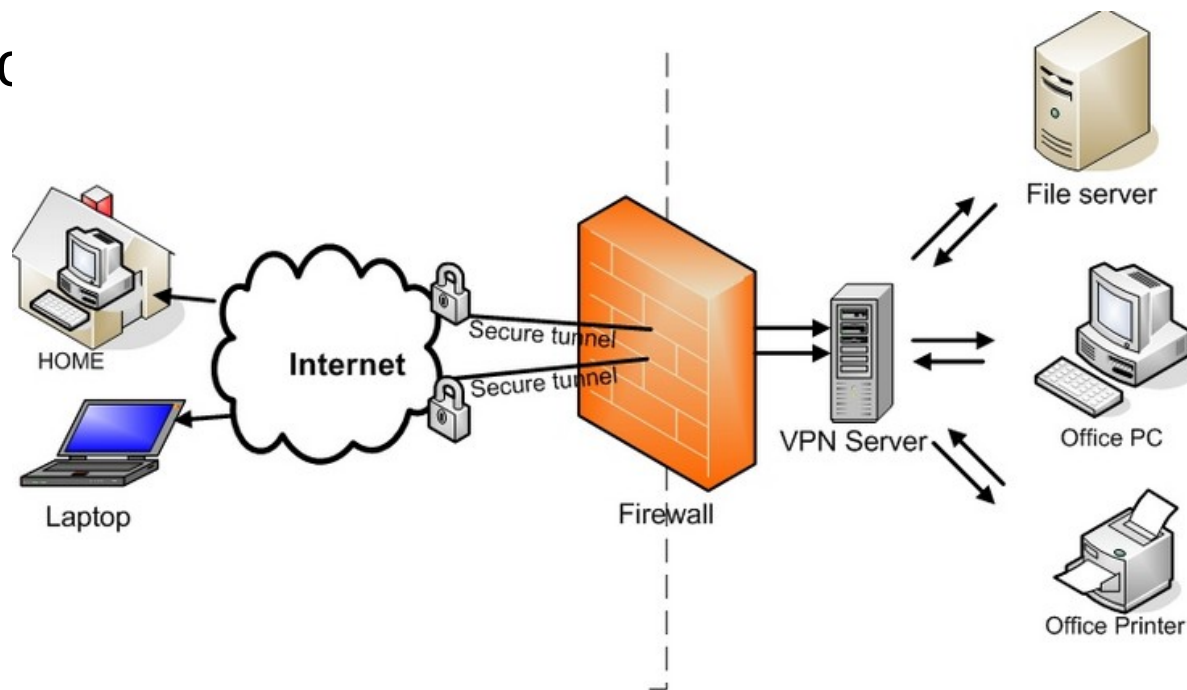


Virtual Private Network

VPN – защищенная логическая сеть, построенная на базе сети с низким уровнем доверия. Строится с использованием криптографических протоколов.

Обычно осуществляет
на сетевом уровне:

- IPSec
- PPTP
- OpenVPN



VPN-сервисы

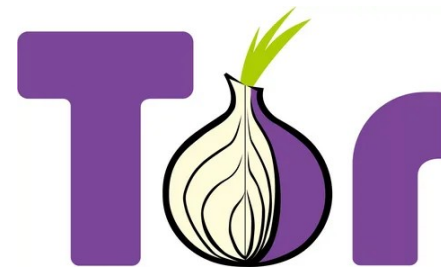
- Поддерживаемые протоколы.
- Возможность выбора точки выхода.
- Ведение логов провайдером, предоставление их третьим лицам.

Цепочка VPN серверов



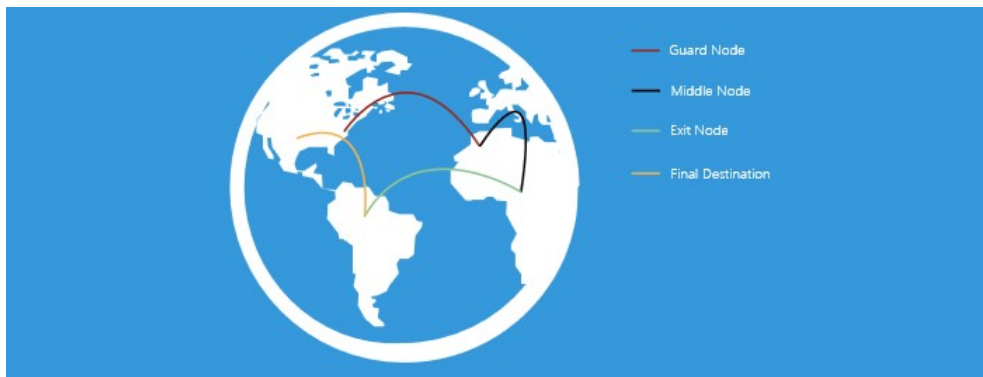
The Onion Router

- 1995г. - начата разработка проекта в Исследовательской лаборатории ВМС США
- 2002г. - опубликован исходный код Tor
- 2004г. - в сети около 20 узлов
- 2008г. - выпуск Tor-браузера
- 2020г. - в сети около 6000 узлов (metrics.torproject.org)



Основные спонсоры: государственный департамент и министерство обороны США.

Промежуточные узлы

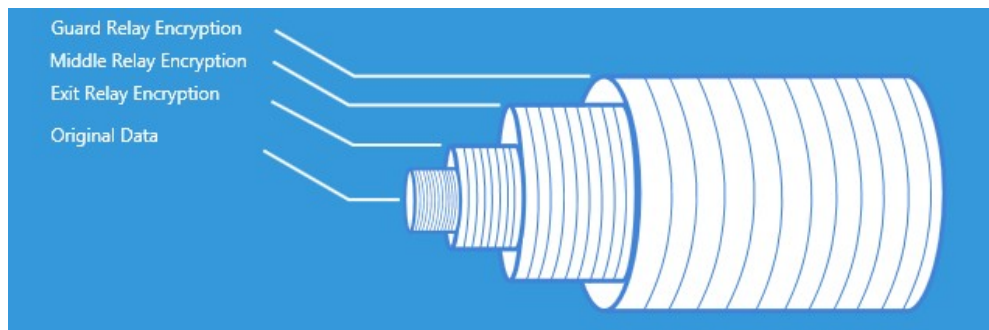


6000 узлов

1000 выходных узлов

10 directory authorities (DA)

2 млн. пользователей



Tor мосты

Мосты – непубликуемые в общем доступе узлы.

Предоставляют проху для доступа в сеть Tor.

Получение адреса моста:

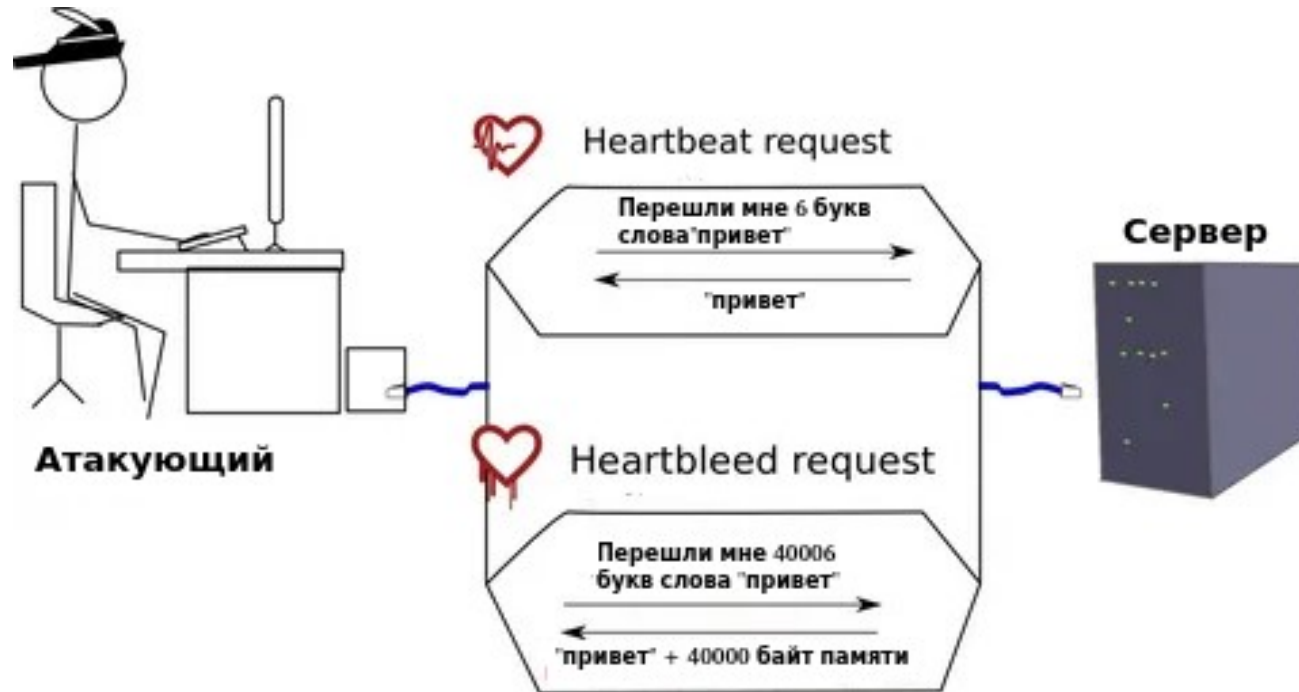
- на сайте bridges.torproject.org
- по почте с bridges@torproject.org

Выходные узлы

Ответственны за действия пользователей сети:

- 2007г. - аресторван Александр Янссен (Германия) по обвинению о ложном сообщении о теракте.
- 5.04.2017г. - арестован Дмитрий Богатов по обвинению в призывах к терроризму и организации массовых беспорядков.
- 11.02.2018г. задержан Дмитрий Клепиков по схожему обвинению.

Heartbleed



14 декабря 2012 г. - распространилась с OpenSSL 1.0.1

1 апреля 2014 г. - официально сообщили об ошибке

CVE-2020-0601

Доверенные сертификаты
от Windows в:
Windows10, Windows Server
2016 и Windows Server
2019:

$(OK_1, (E_1, P_1))$

$(OK_2, (E_2, P_2))$

$(OK_3, (E_3, P_3))$

Проверка сертификата:

должно быть:

if $(OK_1, (E_1, P_1)) == (OK_2, (E_2, P_2))$
then равны

реализовано:

if $OK_1 == OK_2$
then равны

<https://sesc-infosec.github.io/>