

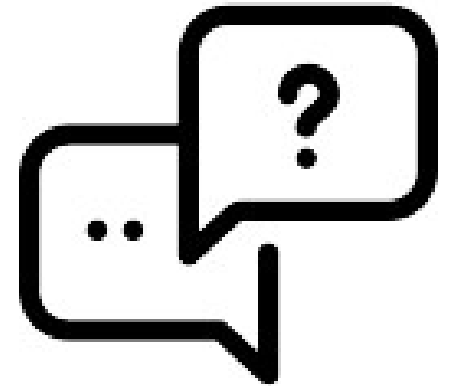
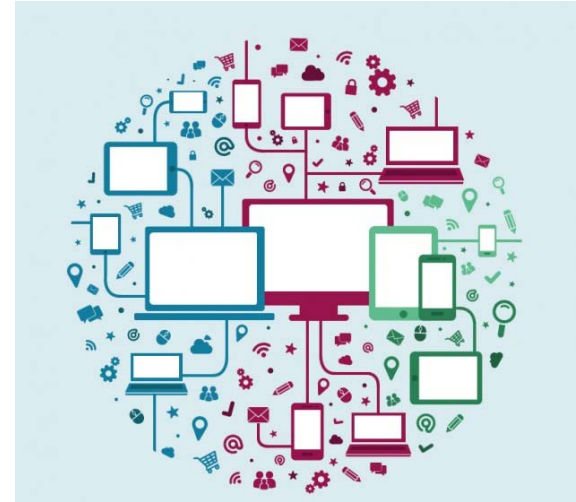
Компьютерные сети

# Прикладной уровень

Как работают протоколы прикладного уровня и чем они отличаются от TCP/UDP.

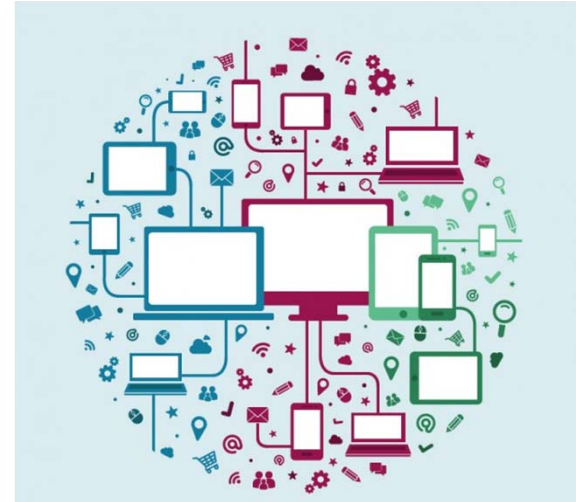
# Вопросы к аудитории

1. Проверка домашних работ.
2. Есть ли проблемы?



# План урока

- Основы сетевой безопасности
- VPN и их назначение
- Основы работы протоколов 7 уровня модели OSI





# Сетевая безопасность

**Сетевая безопасность** - прикладная научная дисциплина, занимающаяся вопросами обеспечения информационной безопасности компьютерной сети и её ресурсов.

Сетевая безопасность включает в себя набор правил, методик и средств обеспечивающих надежность и конфиденциальность передачи информации в сети.





# Примеры сетевых атак

- Перехват трафика
- ARP spoofing
- Сканирование TCP портов



# Шифрование

Существует два типа алгоритмов шифрования:

- **симметричный** — такой тип шифрования при котором для шифровки и дешифровки используется один и тот же ключ
- **асимметричный** — такой тип шифрования, при котором для шифровки и дешифровки используются **пара ключей закрытый/открытый**.
  - **открытый ключ** — зашифровывает и передаётся открыто
  - **закрытый ключ** — расшифровывает и **НЕ** передаётся



# SSL/TLS

**Secure sockets layer** (уровень защищённых сокетов) - криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

Стоит отметить, что основная работа шифрования данных **TLS** и **SSL** проходит на **6** уровне модели **OSI** (уровень представления), а аутентификация — на **5** уровне модели **OSI** (сеансовый уровень)





# VPN

**VPN (Виртуальная частная сеть)** – это набор технологий для создания туннеля между двумя сетевыми устройствами. Протоколы, реализующие VPN дополнительно могут выполнять следующие функции:

- Шифрование трафика
- Аутентификация источника и передатчика
- Проверка достоверности данных
- Защита от подмены данных путем повторной передачи





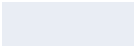


# Классификация VPN

Существует два типа VPN туннелей:

- **Remote access VPN** – означает, что туннель организуется между приложением на компьютере клиента и каким-либо устройством, которое выступает в качестве сервера
- **Site-to-site VPN** – подразумевает наличие двух устройств (например, маршрутизаторов), между которыми имеется перманентный туннель





# Протоколы используемые для построения сетевых туннелей:

- GRE
- PPTP
- L2TP
- OpenVPN
- IPSec





# IPsec

**IPsec** - наиболее широко используемый протокол для построения VPN.

IPsec является набором протоколов:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Security Association and Key Management Protocol (ISAKMP)



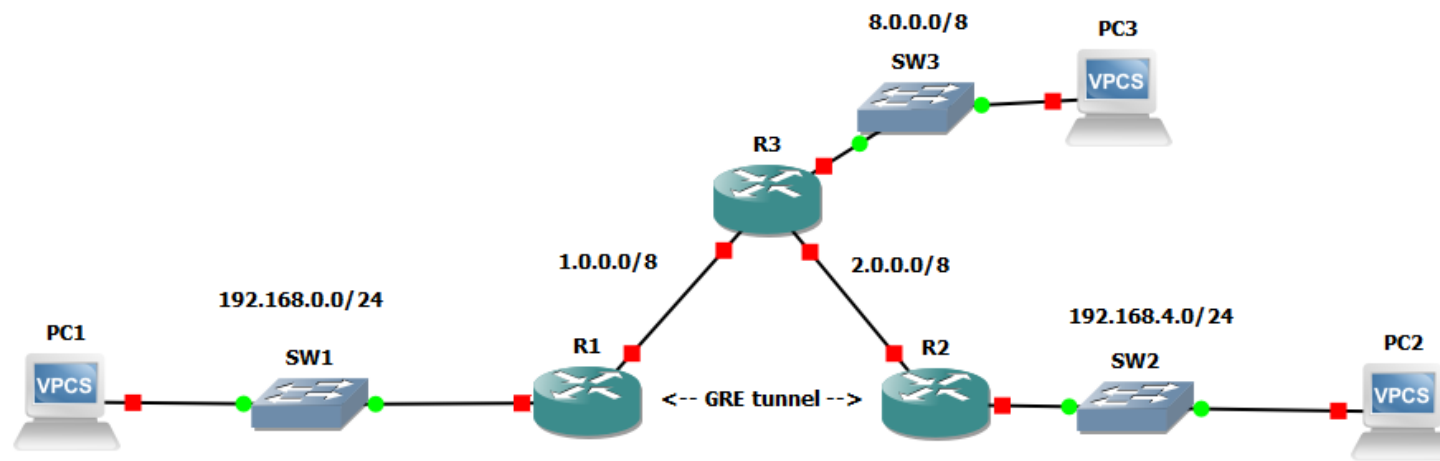


# GRE

**GRE (Generic Routing Encapsulation)** – протокол инкапсуляции, который широко применяется как сам по себе, так и в совокупности с IPSec для создания туннелей.



# GRE - тоннель





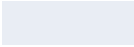
# Прикладной уровень

Произвольное общение между двумя хостами, это может быть как передача запросов от клиента к серверу/передача ответов от сервера к клиенту, так и просто передача/приём произвольных байтов данных между хостами, к примеру – передача файлов.

Протоколы прикладного уровня:

- HTTP, DNS, POP3, IMAP, SMTP,
- SNMP, Telnet, SSH,
- FTP, TFTP, RDP, iSCSI,
- RTP, NTP.





# WEB протоколы: HTTP/HTTPS

**Hyper Text Transfer Protocol** — это протокол передачи гипертекстовых документов. Один из наиболее распространенных протоколов используемых в сети.

Порт/ID: TCP/80

**HyperText Transfer Protocol Secure** — это безопасная версия протокола HTTP с расширением, использующая протоколы шифрования SSL или TLS, для безопасной передачи данных.

Порт/ID: TCP/443



# Основные понятия HTTP

**HyperText Transfer Protocol** (протокол передачи гипертекста) — протокол прикладного уровня осуществляющий передачу структурированных данных в формате HTML. Также протокол позволяет передавать произвольные данные (документы/картинки/видео/музыку).

Технология является клиент-серверной и использует:

- Веб-сервер
- Браузер/клиентское приложение

http://www.domain.com:1234/path/to/resource?a=b&x=y

The diagram illustrates the components of the URL `http://www.domain.com:1234/path/to/resource?a=b&x=y` using red horizontal lines and vertical labels:

- protocol**: Points to `http`
- host**: Points to `www.domain.com`
- port**: Points to `:1234`
- resource path**: Points to `/path/to/resource`
- query**: Points to `?a=b&x=y`







# Веб сервер

Веб сервер – это понятие может подразумевать аппаратную или программную составляющие.

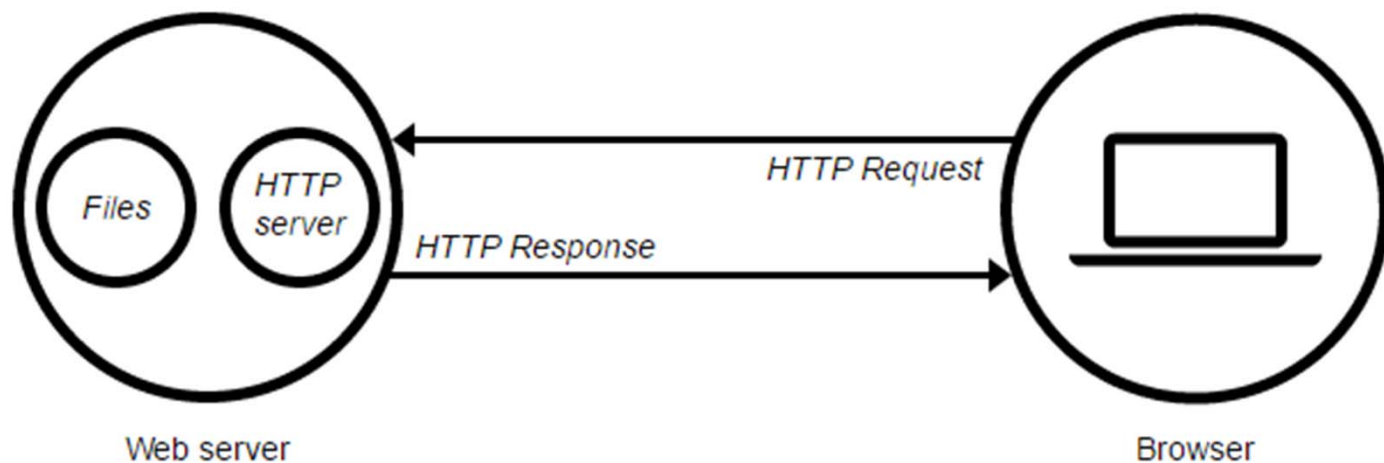
Это компьютер на котором установлено программное обеспечение выполняющие ответы на запросы пользователей.

Веб сервер – это программа принимающая запросы от клиентских программ (браузеров), контролирующая доступ к ресурсам и генерирующая ответы на запросы.



# Работа веб сервера

Когда браузер производит обращение к странице, находящейся на веб сервере, то сервер производит считывание файла или генерацию запрошенного контента и производит передачу контента клиенту.





# Методы HTTP

Существующие методы:

- GET
- POST
- PUT
- DELETE
- HEAD
- TRACE
- OPTIONS





# Коды состояния

1xx: Информационные сообщения

2xx: Сообщения об успехе

3xx: Перенаправление

4xx: Клиентские ошибки

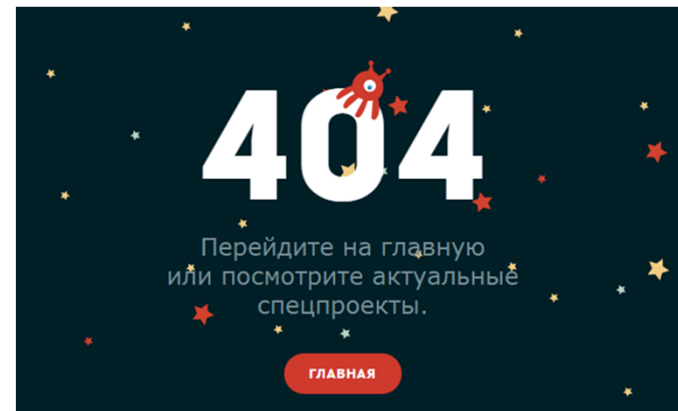
5xx: Ошибки сервера



## Not Found

The requested URL /404 was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.



## Страница не найдена.

Не переживайте, мы уже знаем об ошибке, но будем признательны, если Вы сообщите нам как можно больше подробностей о том, как Вы сюда попали :)

Мы постараемся быстро все поправить.

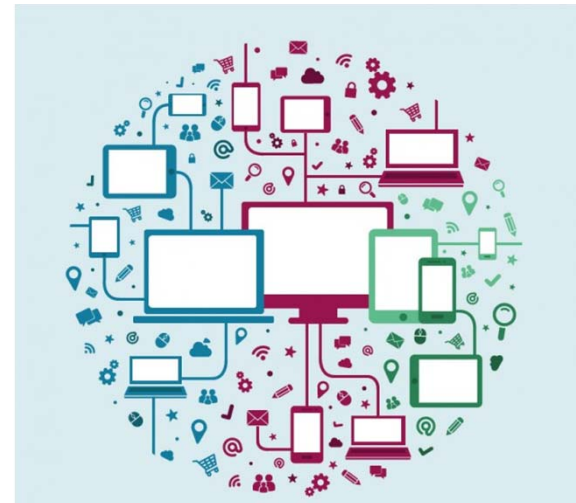
[СООБЩИТЬ ОБ ОШИБКЕ](#)

[← Вернуться на сайт](#)

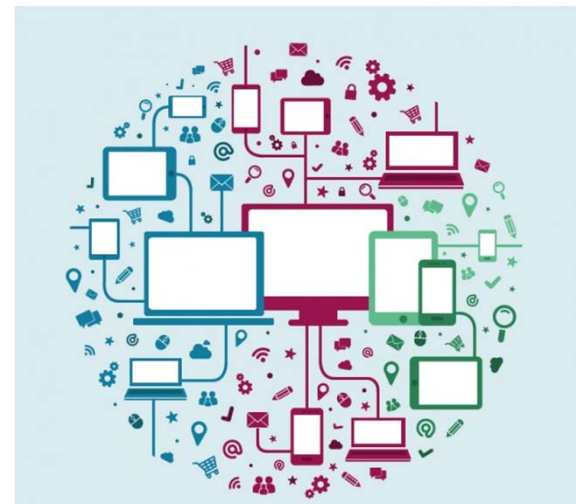


# Домашнее задание

Работа в РТ.



# Вопросы



Есть ли вопросы?

