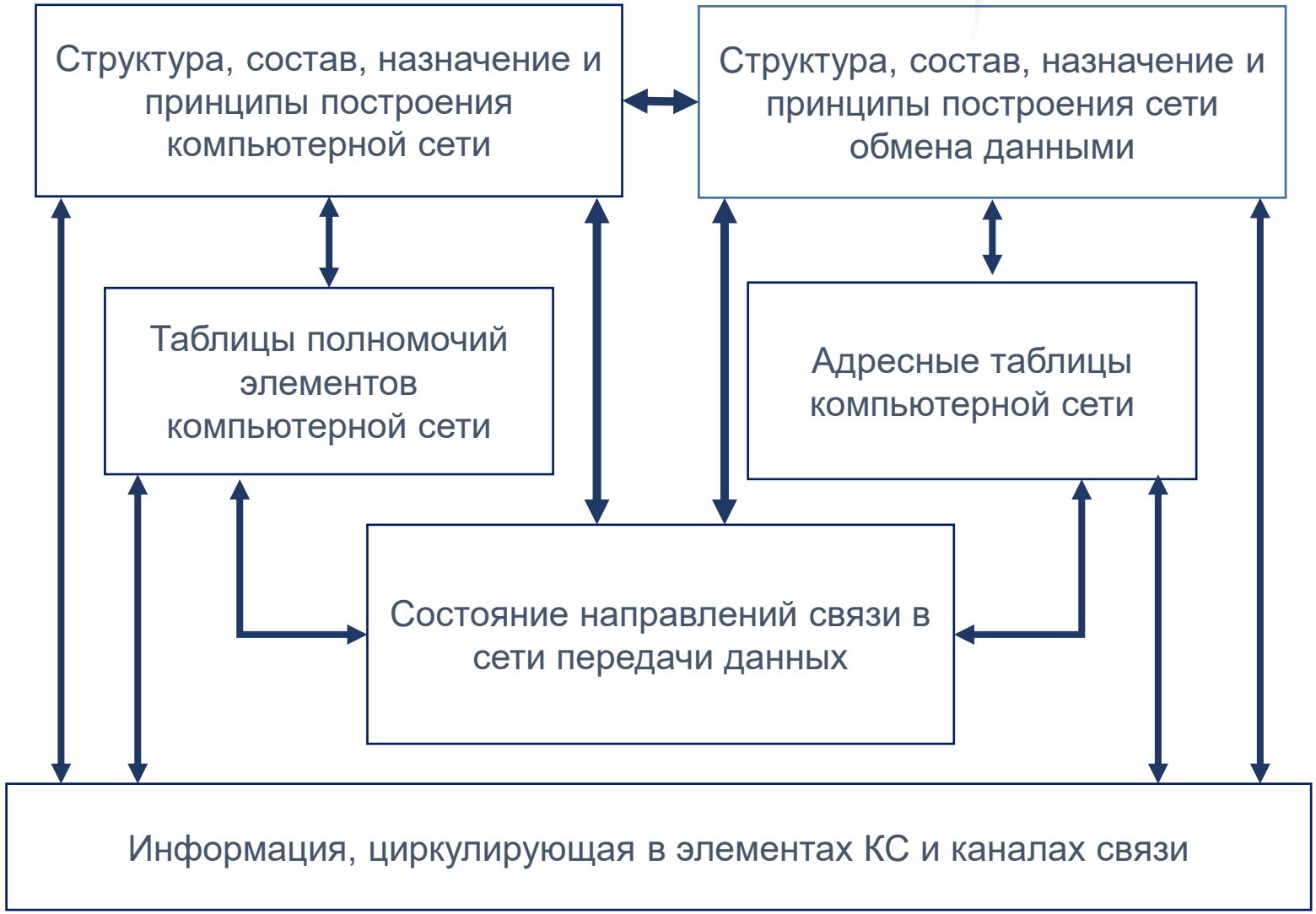
ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Сетевые протоколы передачи информации.
Модель OSI

Многоуровневая система обеспечения защиты



Модель OSI

Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO).

Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашел отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF).

- Модель OSI, которая была определена в серии стандартов ISO/IEC 7498, состоит из следующих частей:
- ISO/IEC 7498-1 — базовая модель;
- ISO/IEC 7498-2 — архитектура безопасности;
- ISO/IEC 7498-3 — наименования и адресация;
- ISO/IEC 7498-4 — система менеджмента.

Модель OSI

Прикладной	Хост, сервер HTTP, FTP, POP3, WebSocket	Заголовок | Данные	Данные
Представительский	ASCII, EBCDIC, JPEG, MIDI	2 | 1 | Данные	Данные
Сеансовый	Межсетевой экран, RPC, PAP, L2TP, gRPC	3 | 2 | 1 | Данные	Сегменты
Траспортный	TCP, UDP	4 | 3 | 2 | 1 | Д	Дейтаграммы
Сетевой	Маршрутизатор IP, ICMP	5 | 4 | 3 | 2 | 1 | Д	Пакеты
Канальный	Коммутатор PPP, IEEE 802.22, Ethernet, DSL, ARP,	6 | 5 | 4 | 3 | 2 | 1 | Д	Кадры
Физический	Кабель, среда передачи	7 | 6 | 5 | 4 | 3 | 2 | 1 | Д	Сигналы

7 | 6 | 5 | 4 | 3 | 2 | 1 | Д

Модель OSI. Физический уровень

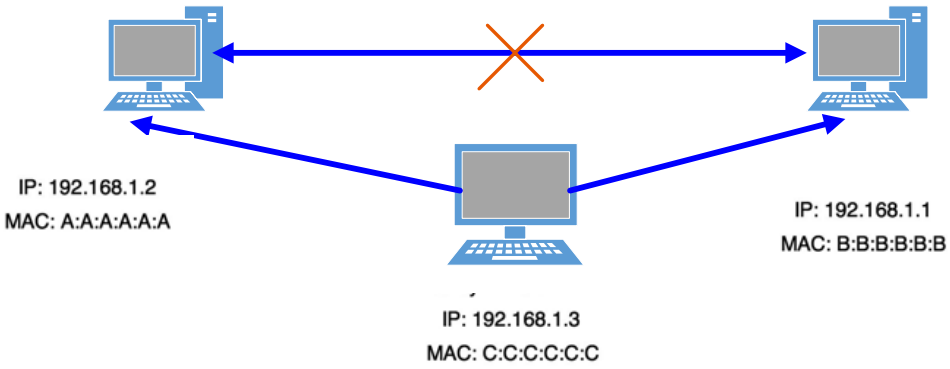
Тип данных	Биты (frame)
Описание уровня	Передача двоичных данных
Основная цель	Кодирование данных в нуль и единицу в качестве сигналов, передаваемые по среде передачи
Характеристики	•Загруженность сети -пропускная способность, измеряемая, в бит/с, то есть, сколько данных мы можем передать за единицу времени. •Задержка, сколько времени пройдет, прежде чем сообщение дойдет от отправителя к получателю.
Канал передачи	•Кабели: телефонный, коаксиал, витая пара, оптический. •Беспроводные технологии, такие как, радиоволны, инфракрасное излучение
Протоколы,	Протоколы 100BaseT, 1000 Base-X
Примеры атак	Физическое разрушение, физическое препятствие работе или управлению физическими сетевыми активами
Последствия	Сетевое оборудование приходит в негодность и требует ремонта для возобновления работы

Модель OSI. Канальный уровень

Тип данных	Кадры
Описание уровня	Установка и сопровождение передачи сообщений на физическом уровне
Основная цель	Кодирование данных в нуль и единицу в качестве сигналов, передаваемые по среде передачи. Задачи: Найти, где в потоке бит, начинается и оканчивается сообщение Обнаружить и скорректировать ошибки. Доставка сообщения адресату. Обеспечение согласованного доступа к разделяемой среде с контролем несущей.
Характеристики	•Загруженность сети -пропускная способность, измеряемая, в бит/с, то есть, сколько данных мы можем передать за единицу времени. •Задержка, сколько времени пройдет, прежде чем сообщение дойдет от отправителя к получателю. •Количество ошибок.
Канал передачи	адаптеры и драйверы, подходящие к ним
Протоколы,	Протоколы 802.3, 802.5
Примеры атак	MAC-флуд — переполнение пакетами данных сетевых коммутаторов
Последствия	Потоки данных от отправителя получателю блокируют работу всех портов

Модель OSI. Сетевой уровень

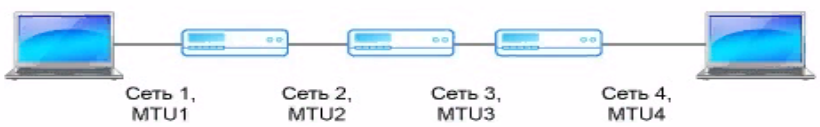
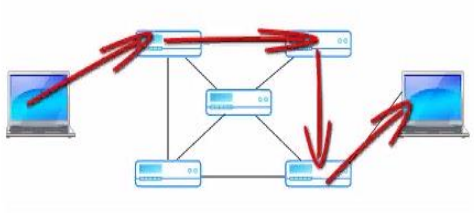
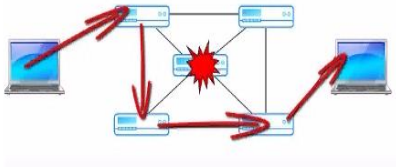
Описание	Защита
Перехват данных с помощью несанкционированного физического подключение к сети	Шифрование данных. Использование интеллектуальных концентраторов для назначения MAC-адресов, имеющих доступ к сети за счет проверки, аутентификации, авторизации и учета на сервере (протокол AAA) Автосегментация-способность изолировать работающие порты, создающие помехи, ошибки или имеющих недопустимый для данной сети MAC-адрес.
Прослушивание сети	Аналогично методам защиты при перехвате.
Наличие коллизий и ошибок и электромагнитных наводок	Кодирование информации Заземление линий передач данных



Модель OSI. Сетевой уровень

Тип данных	Пакеты
Описание уровня	Маршрутизация и передача информации между различными сетями
Основная цель	Обеспечивает процесс логической маршрутизации. **Задачи**: Определение сетевых адресов. Маршрутизация пакетов Фрагментация пакетов. Формирование сообщений об ошибках
Характеристики	•Загруженность сети -пропускная способность, измеряемая, в бит/с, то есть, сколько данных мы можем передать за единицу времени. •Задержка, сколько времени пройдет, прежде чем сообщение дойдет от отправителя к получателю. Количество переданных пакетов с полезной нагрузкой, сообщений об ошибках и др.
Оборудование	Роутеры и коммутаторы L3 уровня
Протоколы,	Протоколы IP, ICMP, ARP, RIP
Примеры атак	ICMP-флуд — DDos-атаки на третьем уровне модели OSI, которые используют ICMP-сообщения для перегрузки пропускной способности целевой сети
Последствия	Снижение пропускной способности атакуемой сети и возможная перегруженность брандмауэра

Модель OSI. Сетевой уровень

Задачи	Атаки
Обеспечение процесса логической маршрутизации 	Фальсификация IP-адреса (спуфинг)
Определение сетевых адресов. Маршрутизация пакетов 	Сканирование сети Атаки на протоколы маршрутизации
Формирование сообщений об ошибках 	Фальсификация IP-адреса (спуфинг)
Фрагментация	Использование туннелирования для передачи трафика в обход системы фильтрации пакетов

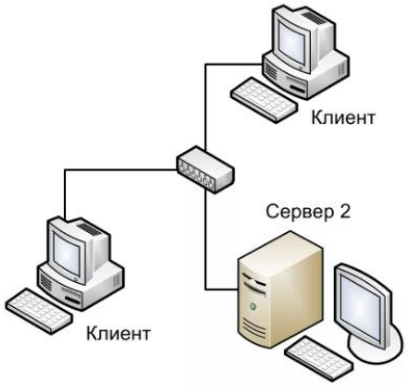
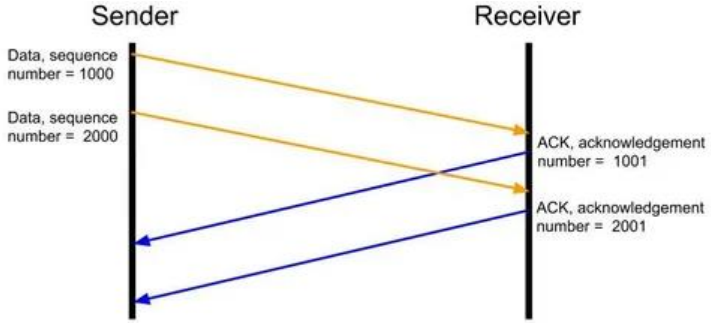
Модель OSI. Защита сетевого уровня

Описание	Защита
Сканирование сети	NAT Использование антиснифферов и средств обнаружения атак (IDS) Закрытие неиспользуемых портов
Атаки на протоколы маршрутизации	Межконцевое шифрование (VPN) Использование механизмов аутентификации на маршрутизаторах (партнеров сетевого взаимодействия, ЦП, привязка к сетевым адресам)
Использование туннелирования для передачи трафика в обход системы фильтрации пакетов	Использование средств обнаружения атак (IDS)
Фальсификация IP-адреса (спуфинг)	Межконцевое шифрование (VPN)

Модель OSI. Транспортный уровень

Тип данных	Сегменты
Описание уровня	Мультиплексирование данных означает, что транспортный уровень способен одновременно обрабатывать несколько потоков данных (потоки могут поступать и от различных приложений) между двумя системами.
Основная цель	Обеспечение гарантированной доставки данных процесс. **Задачи**: Предварительная установка соединения Гарантия доставки данных за счет подтверждение получения Повторная передача
Характеристики	Количество переданных пакетов с полезной нагрузкой, установленными флагами SYN, ACK, FIN, сегментов с повторной передачей. сообщений об ошибках и др.
Оборудование	Используются порты хостов, серверов
Протоколы,	Протоколы TCP, UDP
Примеры атак	SYN-флуд, Smurf-атака (атака ICMP-запросами с измененными адресами)
Последствия	Достижение пределов по ширине канала или по количеству допустимых подключений, нарушение работы сетевого оборудования

Модель OSI. Транспортный уровень

Задачи	Атаки
Установление и разрыв транспортных соединений 	SYN-флуд
	Сканирование портов
Подтверждение получения 	Атака на затопление сети с формированием потока данных о недоставленных пакетах
	Атаки TCP reset

Модель OSI. Защита транспортного уровня

Описание	Защита
Сканирование портов	NAT Закрытие не используемых портов Использование механизмов аутентификации (привязка к портам)
DDos (SYN-flood)	Использование средств обнаружения атак (IDS) и систем мониторинга сетевого трафика
Атака на затопление сети с формированием потока данных о недоставленных пакетах	Оценка производительности сети Использование механизмов балансировки

Модель OSI. Сеансовый уровень

Тип данных	Данные
Описание уровня	Управление установкой и завершением соединения, синхронизацией сеансов связи в рамках операционной системы через сеть
Основная цель	Обеспечение установки и завершения соединения. **Задачи**: Установление и завершение на сеансовом уровне соединения; Выполнение нормального и срочного обмена данными между прикладными процессами; Управление взаимодействием прикладных процессов; Синхронизация работы сеансовых соединений;
Характеристики	Размер окна, объем оперативной памяти, скорость передачи прикладному процессу
Оборудование	Используются оперативную память хостов, серверов
Протоколы	Протоколы X.225, SCP, RPC, PAP
Примеры атак	Увеличение скользящего окна и принудительная передача данных
Последствия	Достижение пределов по объему памяти, недоступность передачи данных для пула пользователей сервиса

Модель OSI. Защита сеансового уровня

Описание	Защита
Увеличение скользящего окна	Учет загрузки ОП при формировании размера скользящего окна
Срочный обмен данными между прикладными процессами	Традиционный подход – фиксированный размер 8 сегментов TCP Предложенный подход – динамический размер окна в зависимости от нагрузки на сеть

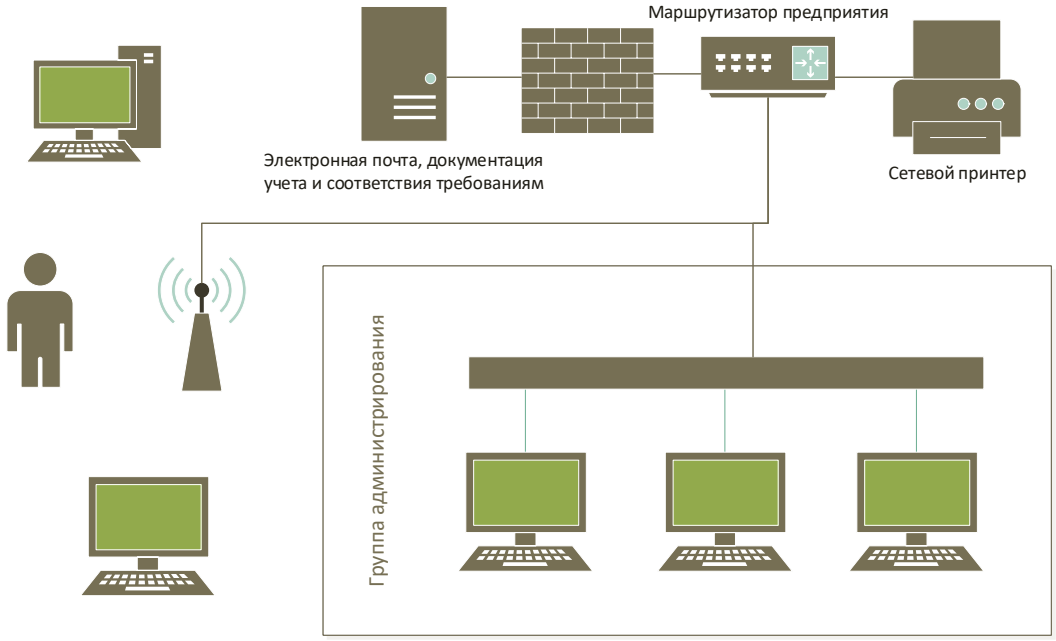
Модель OSI. Представительский уровень

Тип данных	Данные
Описание уровня	Описывает в нужной форме данные, передаваемые между прикладными процессами
Основная цель	**Задачи**: Обеспечение работы с синтаксисом данных, определяя структуру команд, сообщений и ответов. Согласование между прикладными процессами видов представления данных; Реализация форм представления данных; Представление графических , аудио и видео материалов.
Характеристики	Размер данных, синтаксис, форматы данных
Оборудование	Используются оперативную память хостов, серверов
Протоколы	Протоколы сжатия и кодирования данных (ASCII, EBCDIC)
Примеры атак	Переполнение буфера
Последствия	Достижение пределов по объему памяти, недоступность передачи данных для пула пользователей сервиса

Модель OSI. Прикладной уровень

Тип данных	Данные
Описание уровня	Обеспечивает обработку данных для нужд пользователя и прикладные процессы средствами доступа к области взаимодействия
Основная цель	**Задачи**: Описание форм и методов взаимодействия прикладных процессов; Выполнение различных видов операций с данными; Идентификация и аутентификация пользователей; Определение достаточности ресурсов; Синхронизация взаимодействия прикладных процессов; Определение качества обслуживания; Соглашение об исправлении ошибок и определении достоверности данных.
Характеристики	Количество запросов, скорость их обработки, обновление данных
Оборудование	Используются оперативную память хостов, серверов
Протоколы	FTP, HTTP, POP3, SMTP, SSL
Примеры атак	HTTP-flood, SQL инъекция, подбор паролей.
Последствия	Нехватка ресурсов. Чрезмерное потребление системных ресурсов службами на атакуемом сервере (SMTP)

Модель OSI. Прикладной уровень



Вопрос:
Кто относится к внутренним нарушителям информационной безопасности?

- клиенты;
- любые лица, находящиеся внутри контролируемой территории;
- посетители;

Подбор паролей, ключей, атаки типа маскарад
Вирусные, спам– атаки, в том числе переполнение почтового сервера
Атаки отказ в обслуживании
Атаки направленные на «дырки» в программном обеспечении
SQL-инъекции, фишинговые атаки

Модель OSI. Защита прикладного уровня

Описание	Защита
Подбор паролей, ключей, атаки типа маскарад	Криптографическое преобразование; Использование механизмов идентификации и аутентификации;
Вирусные, спам– атаки	Контроль за участниками взаимодействия; Антивирусная защита;
Атаки отказ в обслуживании	Использование средств обнаружения атак (IDS), мониторинг, использование механизмов управление доступом (в.т. ч. МЭ, фильтрация трафика)
Атаки направленные на «дырки» в программном обеспечении	Системное администрирование (в т.ч., анализ log-файлов, установка заплат на ОС и т.д)
SQL-инъекции	Тестирование на проникновение