Практическое занятие №7 Роль файрволов в проблематике сетевой безопасности

Подготовил: Ковалев М.А.

Цель презентации:

- Указать роль файрволов в проблематике сетевой безопасности

Задачи:

- Разобрать Модель ISO/ OSI и стек протоколов TCP/IP
- Указать функции межсетевых экранов

Стек протоколов TCP/IP.

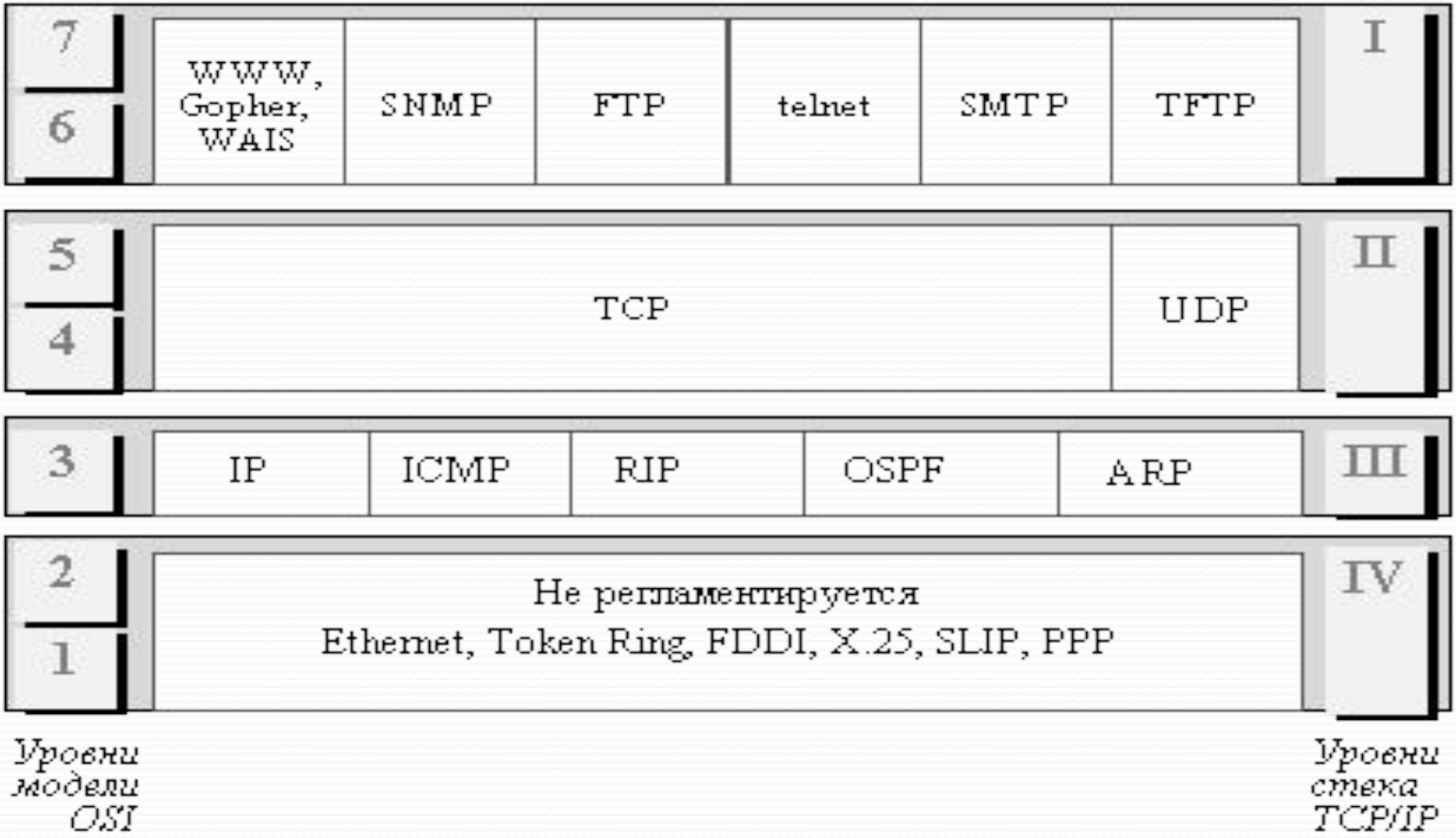
Transmission Control Protocol/Internet Protocol (TCP/IP) - это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Стек был разработан по инициативе Министерства обороны США (Department of Defence, DoD) более 20 лет назад для связи экспериментальной сети ARPAnet с другими сателлитными сетями как набор общих протоколов для разнородной вычислительной среды.

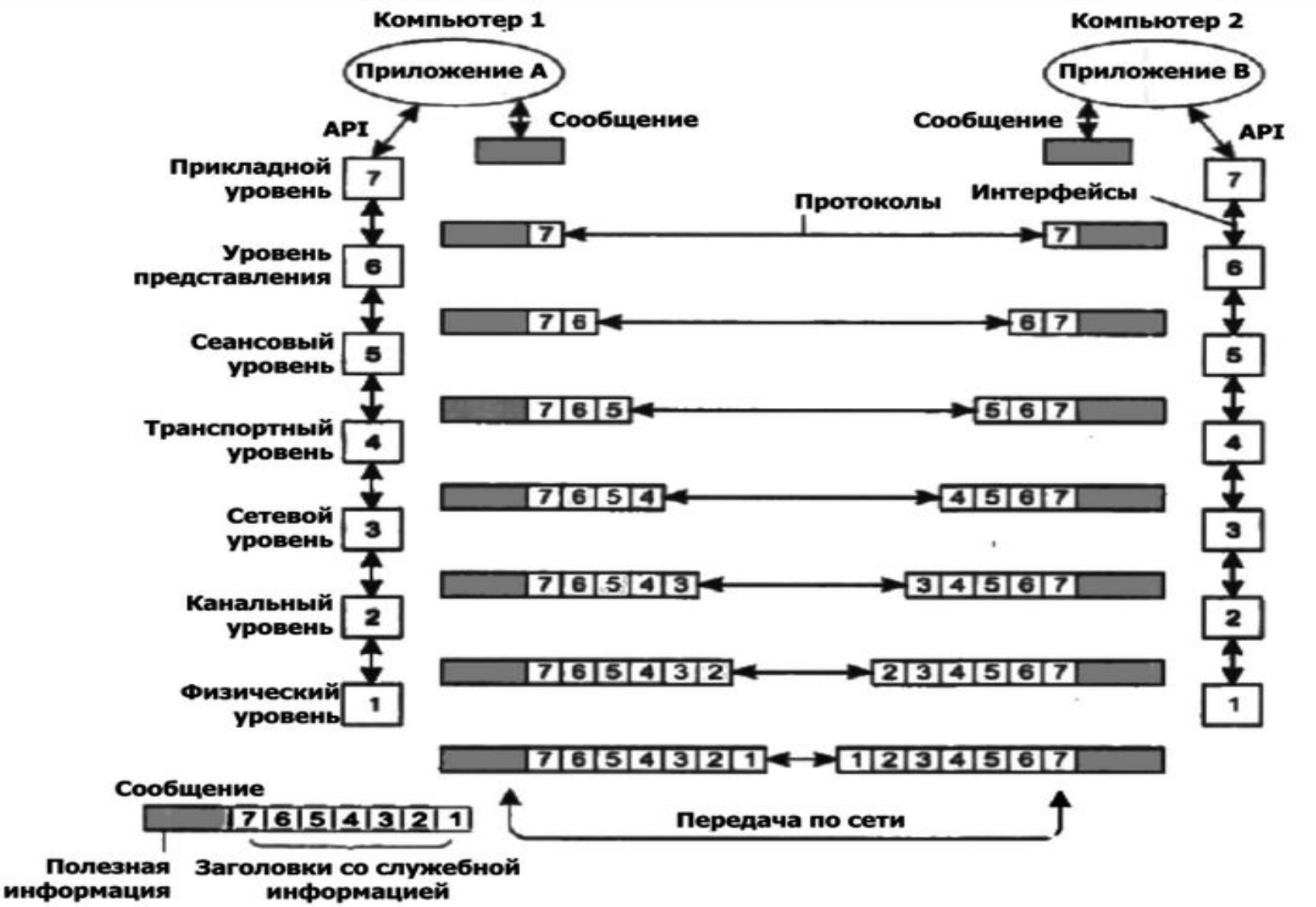
Итак, лидирующая роль стека TCP/IP объясняется следующими его свойствами:

- Это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю.
- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
- Это метод получения доступа к сети Internet.
- Этот стек служит основой для создания intranet- корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet.
- Все современные операционные системы поддерживают стек TCP/IP.
- Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-серве

Структура стека TCP/IP



Модель ISO/ OSI



Анализ угроз информационной безопасности.

Под угрозой понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам.

Классификация возможных угроз информационной безопасности АС может быть проведена по следующим базовым признакам:

1. По природе возникновения
2. По степени преднамеренности проявления
3. По непосредственному источнику угроз
4. По положению источника угроз
5. По степени зависимости от активности АС
6. По степени воздействия на АС
7. По этапам доступа пользователей или программ к ресурсам АС

Функции межсетевых экранов.

Межсетево́й экра́н, сетево́й экра́н — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

МЭ, защищающий сразу множество узлов внутренней сети, призван решить:

• задачу ограничения доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых МЭ;

• задачу разграничения доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

Функции межсетевых экранов

До сих пор не существует единой общепризнанной классификации МЭ. Их можно классифицировать, например, по следующим основным признакам:

- По функционированию на уровнях модели OSI:
  - пакетный фильтр (экранирующий маршрутизатор — screening router);
  - шлюз сеансового уровня (экранирующий транспорт);
  - прикладной шлюз (application gateway);
  - шлюз экспертного уровня (stateful inspection firewall).

- По используемой технологии:
  - контроль состояния протокола (stateful inspection);
  - на основе модулей посредников (proxy).

- По исполнению:
  - аппаратно-программный;
  - программный.

- По схеме подключения:
  - схема единой защиты сети;
  - схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
  - схема с раздельной защитой закрытого и открытого сегментов сети.

Основные функции подсистемы защиты ОС.

1. Разграничение доступа. (Каждый пользователь системы имеет доступ только к тем объектам операционной системы, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.)
2. Идентификация и аутентификация. (Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, за кого он себя выдает.)
3. Аудит. (Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.)

Выводы:

- Разобрали Модель ISO/ OSI и стек протоколов TCP/IP
- Указали функции межсетевых экранов