**Лекция 12.**

**Аудит угроз сетевых атак согласно уровням модели OSI**

Эталонная модель взаимодействия открытых систем OSI (Open Systems Interconnection) была разработана институтом стандартизации ISO с целью разграничить функции различных протоколов в процессе передачи информации от одного абонента другому. Подобных классов функций было выделено 7 – они получили название уровней (рис. 1)

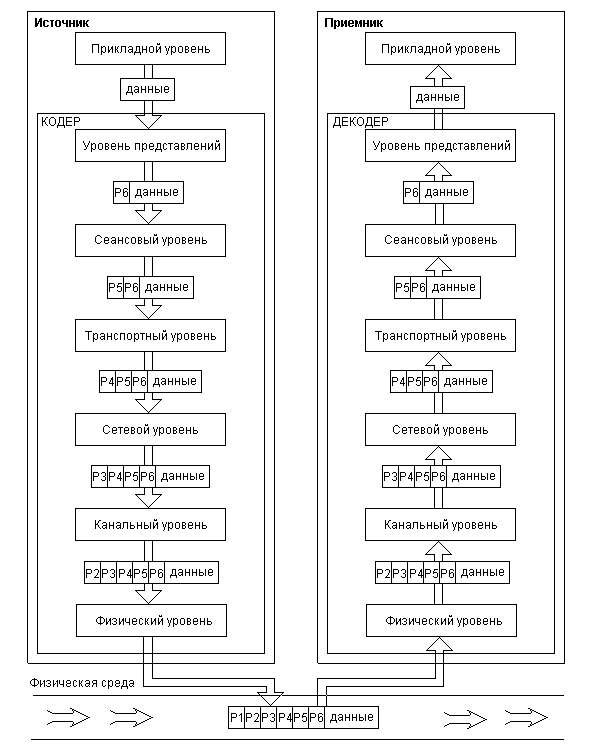


Рисунок 1 – Уровни модели OSI

Каждый уровень выполняет свои определенные задачи в процессе передачи блока информации, причем соответствующий уровень на приемной стороне производит преобразования, точно обратные тем, которые производил тот же уровень на передающей стороне. В целом прохождение блока данных от отправителя к получателю показано на рис.1. Каждый уровень добавляет к пакету небольшой объем своей служебной информации – префикс (на рисунке они изображены как P1...P7). Некоторые уровни в конкретной реализации вполне могут отсутствовать. На рис. 2 показаны логические соединения между уровнями.

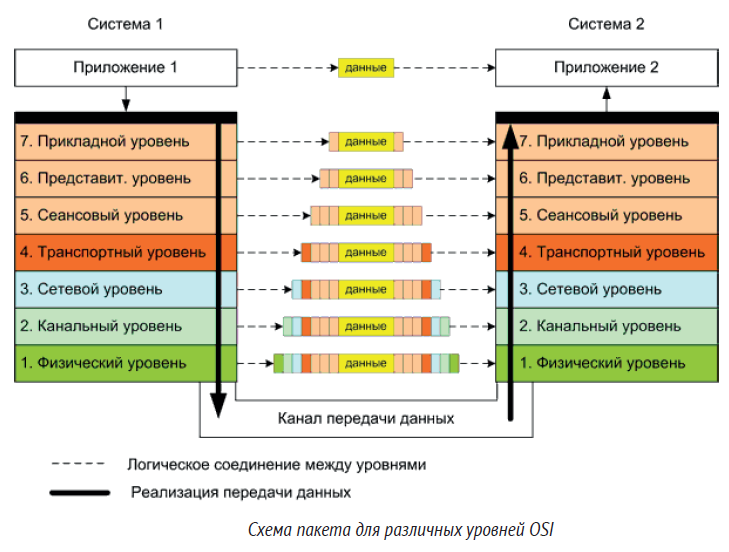


Рисунок 2 – Логические соединения уровней OSI

Аудит угроз сетевых атак согласно базируется на данной модели и позволяет оценить и классифицировать сетевые атаки согласно уровню их воздействия.

Физический уровень отвечает за преобразование электронных сигналов в сигналы среды передачи информации (импульсы напряжения, радиоволны, инфракрасные сигналы). На этом уровне основным классом атак является "отказ в сервисе". Постановка шумов по всей полосе пропускания канала может привести к "надежному" разрыву связи.

Канальный уровень управляет синхронизацией двух и большего количества сетевых адаптеров, подключенных к единой среде передачи данных. Примером его является протокол EtherNet. Воздействия на этом уровне также заключаются в основном в атаке "отказ в сервисе". Однако, в отличие от предыдущего уровня, здесь производится сбой синхропосылок или самой передачи данных периодической передачей "без разрешения и не в свое время".

Сетевой уровень отвечает за систему уникальных имен и доставку пакетов по этому имени, то есть за маршрутизацию пакетов. Примером такого протокола является протокол Интернета IP. Все атаки, основанные на заведомо неправильной маршрутизации пакетов, мы уже рассмотрели.

Транспортный уровень отвечает за доставку больших сообщений по линиям с коммутацией пакетов. Так как в подобных линиях размер пакета представляет собой обычно небольшое число (от 500 байт до 5 килобайт), то для передачи больших объемов информации их необходимо разбивать на передающей стороне и собирать на приемной. Транспортными протоколами в сети Интернет являются протоколы UDP и TCP. Реализация транспортного протокола – довольно сложная задача, а если еще учесть, что злоумышленник придумывает самые разные схемы составления неправильных пакетов, то проблема атак транспортного уровня вполне объяснима.

Все дело в том, что пакеты на приемную сторону могут приходить и иногда приходят не в том порядке, в каком они были отправлены. Причина обычно состоит в потере некоторых пакетов из-за ошибок или переполненности каналов, реже – в использовании для передачи потока двух альтернативных путей в сети. А, следовательно, операционная система должна хранить некоторый буфер пакетов, дожидаясь прихода задержавшихся в пути. А если злоумышленник с умыслом формирует пакеты таким образом, чтобы последовательность была большой и заведомо неполной, то тут можно ожидать как постоянной занятости буфера, так и более опасных ошибок из-за его переполнения.

Сеансовый уровень отвечает за процедуру установления начала сеанса и подтверждение (квитирование) прихода каждого пакета от отправителя получателю. В сети Интернет протоколом сеансого уровня является протокол TCP (он занимает и 4, и 5 уровни модели OSI). В отношении сеансового уровня очень широко распространена специфичная атака класса "отказ в сервисе", основанная на свойствах процедуры установления соединения в протоколе TCP. Она получила название SYN-Flood (зд. flood – англ. "большой поток").

При попытке клиента подключиться к серверу, работающему по протоколу TCP (а его используют более 80% информационных служб, в том числе HTTP, FTP, SMTP, POP3), он посылает серверу пакет без информации, но с битом SYN, установленным в 1 в служебной области пакета – запросом на соединение. По получении такого пакета сервер обязан выслать клиенту подтверждение приема запроса, после чего с третьего пакета начинается собственно диалог между клиентом и сервером. Одновременно сервер может поддерживать в зависимости от типа сервиса от 20 до нескольких тысяч клиентов.

При атаке типа SYN-Flood злоумышленник начинает на своей ЭВМ создавать пакеты, представляющие собой запросы на соединение (то есть SYN-пакеты) от имени произвольных IP-адресов (возможно даже несуществующих) на имя атакуемого сервера по порту сервиса, который он хочет приостановить. Все пакеты будут доставляться получателю, поскольку при доставке анализируется только адрес назначения. Сервер, начиная соединение по каждому из этих запросов, резервирует под него место в своем буфере, отправляет пакет-подтверждение и начинает ожидать третьего пакета клиента в течение некоторого промежутка времени (1-5 секунд). Пакет-подтверждение уйдет по адресу, указанному в качестве ложного отправителя в произвольную точку Интернета и либо не найдет адресата вообще, либо чрезмерно "удивит" операционную систему на этом IP-адресе (поскольку она никаких запросов на данный сервер не посылала) и будет просто проигнорирован. А вот сервер при достаточно небольшом потоке таких запросов будет постоянно держать свой буфер заполненным ненужными ожиданием соединений и даже SYN-запросы от настоящих легальных пользователей не будут помещаться в буфер : сеансовый уровень просто не знает и не может узнать, какие из запросов фальшивые, а какие настоящие и могли бы иметь больший приоритет.

Атака SYN-Flood получила довольно широкое распространение, поскольку для нее не требуется никаких дополнительных подготовительных действий. Ее можно проводить из любой точки Интернета в адрес любого сервера, а для отслеживания злоумышленника потребуются совместные действия всех провайдеров, составляющих цепочку от злоумышленника до атакуемого сервера (к чести сказать, практически все фирмы-провайдеры, если они обладают соответствующим программным обеспечением и квалифицированным персоналом, активно участвуют в отслеживании атакующей ЭВМ по первой же просьбе, в том числе и от зарубежных коллег).