

1.3. Модель сетевой безопасности

Все *атаки* можно разделить на два класса: *пассивные* и *активные*.

I. Пассивная атака

Пассивной называется такая *атака*, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.

II. Активная атака

Активной называется такая *атака*, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы *активных атак*:

1. Отказ в обслуживании - *DoS-атака (Denial of Service)*

Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов. Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения. В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

2. Модификация потока данных - *атака "man in the middle"*

Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

3. Создание ложного потока (фальсификация)

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого.

4. Повторное использование

Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая *replay-атака*. На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.

Перечисленные *атаки* могут существовать в любых типах сетей, а не только в сетях, использующих в качестве транспорта протоколы TCP/IP, и на любом уровне модели OSI.