# Основы противодействия DDoS-атакам

**Ключевые слова:**

DDoS-атака, безопасность, защита, интернет, информационная безопасность, классификация, методы защиты, методы обнаружения, механизмы защиты.

**Аннотации:**

В данной работе рассматриваются основы противодействия DDoS-атакам. Выявлены основные типы DDoS-атак, их подтипы, показаны основные способы противодействия данному типу угрозы. Также приведен пример реализации защиты от DDoS-атаки методом псевдослучайной смены сетевых адресов.

## 1) Введение. DDoS-атаки.

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразное количество запросов, которые не успевает обработать.

**Существует два наиболее значимых типа DDoS-атак.**

Низкоуровневые происходят на транспортном и сетевом уровнях OSI-модели. Они используют несовершенство сетевой архитектуры.

Высокоуровневые осуществляются на сеансовом, представительском и прикладном уровнях. Они эмулируют действия пользователей.

**Подтипы DDoS-атак.**

*Наводнения SYN* атаки происходят на потребности средств сервера в предоставить огромной структуры данных памяти для аутентификации входящих SYN-пакетов. Во время атак SYN flood злоумышленник отправляет большее количество SYN-пакетов на адреса. В процессе ответа на запрос время, когда сервер отправляет информацию запроса в память стек, он будет ждать подтверждения от клиента, что отправляет запрос.

*Smurf* атака типа ICMP Flood, где злоумышленники используют пакеты эхо-запроса ICMP, направленные на IP широковещательные адреса из удаленных мест для генерации атаки отказа в обслуживании.

*HHTP nomon* относится к атаке, которая бомбардирует веб серверы с HTTP-запросами. Чтобы отправить HTTP-запрос, должно быть установлено действующее TCP-соединение, которое требуется подлинный IP-адрес. Злоумышленники могут добиться этого используя IP-адрес бота.

Еще одна важная DDoS-атака — это атака *SIP flood*.

Широко поддерживаемый открытый стандарт настройки вызова в передача голоса по IP (VoIP) - протокол инициирования сеанса (SIP). Как правило, прокси-серверы SIP требуют общедоступного доступа в Интернет для приема запросов на установку вызова от любого клиента VoIP.  Как один из

вариантов атаки, злоумышленники могут затопить SIP-прокси с множеством пакетов SIP INVITE, которые имеют поддельные исходные IP-адреса.

**2) Защита от DDoS-атак**

Защита от DoS и DDoS атак сильно зависит от модели сети и типа атаки. Было предложено несколько механизмов для решения этой проблемы. Методы *переупорядочения* и *улучшения протокола* сделают протоколы безопасности более надежными и менее уязвимыми к атакам на ресурсы жертвы.

*Фильтрация входящего сетевого трафика* — это механизм, предлагаемый для предотвращения атаки, использующий поддельные адреса.

Сообщения *трассировки ICMP* полезны для распознавания пути, по которому проходят пакеты через Интернет.

*IP-трассировка* предлагает надежный способ выполнения поэтапного отслеживания пакета до атакующего источника откуда он возник.

*Детерминированная маркировка пакетов (DPM)* - полагается на информацию вписываемой в заголовок пакета маршрутизаторами при прохождении пакета по сети.

*Вероятностная маркировка пакетов (PPM)* метод, который устраняет подделку IP-адреса, позволяя каждому маршрутизатору вероятностно вписать информацию о локальном пути в пакет, который его проходит.

*PushBack* подходы были предложены для извлечения сигнатуры атак путем ограничения скорости сомнительного трафика предназначенного для перегруженного сети.

*MULTOPS* - маршрутизаторы замечают атаки на полосу пропускания, используя эвристику, основанную на скорости отправки пакетов. Нарушение этого состояния фиксирует DDoS-атаку.

*D-WARD* - выполняет статистическое профилирование трафика на краю сети, чтобы заметить новые типы DDoS-атак.

**3) Методы обнаружения и предотвращения DDoS-атак**

Обнаружение представляет собой один из важнейших факторов при защите от DDoS-атак. Главными критериями качественного метода обнаружения являются малое время работы и низкий процент ложных срабатываний.

Классификация систем обнаружения DDoS-атак основывается на используемом методе обнаружения, таких выделяют два: обнаружение атак на основе сигнатур и на основе аномалий.

Обнаружение атак на основе сигнатур**.** Идентификация на основе сигнатур обычно используется для идентификации известных типов атак. Для обнаружения этих видов атак необходима база данных с известными сигнатурами атак.

Обнаружение атак на основе аномалий**.** Методы обнаружения вторжений, основанные на противоречивости, распознают необычную активность и создают предупреждения аномалий в действиях системы или действиях приложений.

4) **Классификация архитектур предотвращения DDoS-атак в соответствии с местом их развертывания.**

Защитные механизмы от атак типа «отказ в обслуживании» классифицирует в зависимости от места их развертывания.

Механизмы защиты, устанавливаемые на стороне источника атаки. В данном типе механизмов защиты от DDoS средства развернуты на стороне источника атаки, чтобы предотвратить создание DDoS-атак пользователями сети. При таком подходе устройства-источники идентифицируют вредоносные пакеты в исходящем трафике и фильтруют или ограничивают трафик.

Механизмы защиты, устанавливаемые на стороне жертвы атаки**.** Жертва обнаруживает, фильтрует или ограничивает скорость вредоносного входящего трафика на маршрутизаторах сетей жертвы, т. е. сетей, предоставляющих веб-службы.

Механизмы защиты, устанавливаемые на промежуточных маршрутизаторах**.** Любой маршрутизатор в сети может независимо попытаться определить вредоносный трафик и фильтровать или ограничить скорость трафика.

Распределенные или гибридные механизмы защиты**.** Механизмы гибридной защиты развертываются в нескольких местах, таких как источник атаки, жертвы или промежуточные сети, и обычно между точками развертывания осуществляется взаимодействие.

### 5) Пример реализации защиты от DDoS-атаки принципом псевдослучайной смены сетевого адреса внутри сессии

Способ защиты от DDoS-атаки строится следующим образом: DNS-сервер содержит запись об IP-адресе сервера авторизации, чтобы получить доступ к серверу, клиент проходит авторизацию. В случае успеха пользователь устанавливает защищенное соединение с контроллером, по нему передается пул IP-адресов для осуществления прыгающей адресации.

Далее клиент обращается к интернет-ресурсу по «инициальному» адресу, при этом адрес назначения следующего отправляемого пакета определяется терминалом пользователя динамически из полученного пула адресов путем расчета специальной хэш-функции.

Пул IP-адресов формируется из адресов, принадлежащих одному или более высокопроизводительному маршрутизатору в Автономной системе или подсети. Контроллер защищенных сессий сообщает каждому такому роутеру идентификатор новой сессии и адрес клиента, с которым должно поддерживаться эторасширенное соединение. Если при проверке рассчитанный IP-адрес совпадает с адресом назначения принятого пакета, тогда он перенаправляется на реальный адрес Интернет-ресурса, в противном случае сбрасывается.

Основная идея реализации метода заключается в следующем: IP Hopper Manager, осуществляющий управление расширенными защищенными

соединениями, при помощи утилиты Netfilter добавляет новый набор правил в цепочку PREROUTING для каждого роутера, участвующего в поддержке процесса обмена пакетами между сервером и клиентом по алгоритму прыгающей адресации. Этот набор правил осуществляет проверку того, что полученный пакет адресован на корректный виртуальный IP-адрес сервера. Если поле адреса назначения удовлетворяет этому условию, то пакет перенаправляется на физический адрес защищаемого сервера, иначе пакет отбрасывается.

Таким образом, данный метод заключается в создании огромного количества IP-адресов, среди которых скрывается реальный IP-адрес сервера, благодаря чему DDoS-атака распределяется сразу на множество потоков, сводя эффективность атаки к минимуму.

## 6) Заключение

В данной работе была проанализирована одна из самых актуальных на сегодняшний день разновидностей хакерских атак – DDoS. Были разобраны наиболее известные типы данных атак, стратегия защиты от них и своевременное обнаружения таких попыток несанкционированного доступа, предотвращения их, а также показан пример одного из способов реализации защиты от DDoS-атаки методом  псевдослучайной смены сетевого адреса внутри сессии.