А. В. Шевелев
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Сидский**, канд. техн. наук, доцент

МЕХАНИЗМЫ ЗАЩИТЫ ОТ DDOS-АТАК В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

DDoS-атака, или атака на отказ в обслуживании, представляет собой одну из самых распространенных угроз для современных информационных систем. Ее суть заключается в создании чрезмерной нагрузки на сервер или сеть, что приводит к сбоям в работе или полной недоступности ресурса для легитимных пользователей. Атакующие используют распределенные сети зараженных устройств, так называемые ботнеты, с которых одновременно отправляют огромное количество запросов. Это приводит к перегрузке канала передачи данных или исчерпанию вычислительных ресурсов сервера. В связи с этим разработка эффективных механизмов защиты от подобных атак является приоритетной задачей для администраторов сетевой инфраструктуры и разработчиков информационных систем [1].

DDoS-атаки могут развиваться поэтапно. Вначале злоумышленники анализируют потенциальную жертву, выявляя уязвимости и возможные способы их эксплуатации. Затем происходит подготовка атаки, которая включает заражение устройств вредоносным программным обеспечением и создание ботнета. После этого осуществляется непосредственная атака – генерация вредоносных запросов, поступающих на сервер жертвы с множества зараженных устройств. Если атака оказывается недостаточно эффективной, злоумышленники могут скорректировать стратегию, изучить слабые места системы и повторить попытку воздействия.

В зависимости от уровня воздействия в модели OSI различают несколько типов DDoS-атак. На сетевом уровне атака направлена на перегрузку каналов передачи данных. На транспортном уровне злоумышленники используют уязвимости протоколов, что приводит к исчерпанию ресурсов сервера. На уровне приложений атака нацелена на эксплуатацию слабых мест в архитектуре веб-приложений и сервисов. Существует также классификация по способу воздействия, согласно которой выделяют атаки, использующие уязвимости протоколов, атаки, создающие чрезмерный поток запросов, а также атаки, направленные на эксплуатацию архитектурных недостатков программного обеспечения.

Современные механизмы защиты от DDoS-атак можно разделить на несколько категорий. В зависимости от принципа работы они могут быть развернуты локально, размещены в облаке или представлять собой гибридные решения, сочетающие оба подхода. Также различают защиту, ориентированную на фильтрацию пакетов на низких уровнях модели OSI, и защиту, направленную на анализ запросов на уровне приложений. Кроме того, существуют технологии симметричной и асимметричной фильтрации трафика, каждая из которых имеет свои преимущества в зависимости от характера атакующего воздействия.

Одним из ключевых аспектов обеспечения безопасности является выбор решений, которые соответствуют уровню угроз. Для защиты на сетевом уровне применяются механизмы фильтрации пакетов, которые позволяют отсекать аномальный трафик, не допуская его прохождения к серверу. В случае атак на уровне приложений необходимо использование более сложных алгоритмов, способных анализировать поведение пользователей и отличать легитимные запросы от вредоносных. Наиболее сложные интеллектуальные атаки требуют применения специализированных инструментов, таких как межсетевые экраны для веб-приложений, которые способны выявлять и блокировать даже самые изощренные методы воздействия.

Выбор эффективных способов защиты зависит от специфики информационной системы. Для минимизации рисков необходимо проводить регулярные тестирования на

уязвимости, а также анализировать возможные сценарии атак. Разработка архитектуры сервисов с учетом потенциальных угроз позволяет существенно повысить уровень защищенности. Однако даже наличие защитных систем не всегда гарантирует полную безопасность. Одним из важнейших факторов является концепция защищаемости, которая предполагает комплексный подход к защите, начиная с проектирования инфраструктуры и заканчивая постоянным мониторингом угроз и адаптацией защитных механизмов.

Таким образом, борьба с DDoS-атаками требует применения многоуровневых стратегий, включающих анализ трафика, фильтрацию вредоносных запросов и использование интеллектуальных систем обнаружения угроз. Комплексный подход к безопасности требует не только применения технических средств, но и разработки стратегий реагирования на инциденты. Важным элементом защиты является организация системы мониторинга, позволяющей оперативно выявлять атаки, а также создание плана аварийного восстановления, который позволит минимизировать возможные последствия атак и обеспечить стабильную работу информационных систем даже в условиях интенсивного кибервоздействия.

Литература

1. Средства и методы защиты от DDoS-атак [Электронный ресурс]. – Режим доступа : https://stormwall.pro/resources/blog/metody-zashchity-ot-ddos-atak. − Дата доступа : 28.03.2024.