УДК 004.056.53

Лян Антон,
Читинский институт
Байкальского государственного университета
г. Чита, Российская Федерация

Бурцева А.Е.,
Читинский институт
Байкальского государственного университета
г. Чита, Российская Федерация

DDoS-атака как игра: поиск равновесия между участниками

В условиях стремительного роста масштабов и сложности DDoS-атак возникает прямая угроза ключевому принципу информационной безопасности – доступности ресурсов, DDoS-атаки перестали быть «фоном» – они стали самостоятельным инструментом информационного и цифрового давления. Традиционные методы защиты требуют рассмотрения с позиций взаимодействия сторон. Применение аппарата теории игр позволяет формализовать конфликт интересов трех ключевых участников – провайдера, пользователя, хакера, – в виде матричной игры с ненулевой суммой, где выигрыши сторон слабо связаны, а поиск равновесия Нэша дает основу для выбора оптимальных защитных стратегий.

Ключевые слова: DDoS-атака, теория игр, равновесие Нэша.

Развитие цифровых сервисов и значительное увеличение числа интернет-пользователей приводит к тому, что все больше «негативных» участников сети пытаются нарушить взаимодействие путем организации большого числа фальшивых запросов. Причины этого кроются как в обычной конкуренции, так и в более сложных мотивах – шантаж, диверсия, хулиганство, политический активизм.

Распределенная атака типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) представляет собой злонамеренную попытку нарушить нормальную работу сервера, сети или веб-приложения путем перегрузки цели вредоносным трафиком, генерируемым множеством одновременно действующих и скоординированных источников. В отличие от классической DoS-атаки, исходящей от одного узла, распределенный характер позволяет злоумышленнику многократно усиливать воздействие и затруднять фильтрацию трафика, поскольку запросы поступают с тысяч и миллионов легитимных IP-адресов.

Угроза в форме DDoS-атак демонстрирует тенденцию к быстрому росту. Согласно данным провайдера Selectel[1], в первом полугодии 2026 г. общее количество отраженных атак на облачную инфраструктуру российских компаний достигло 88 618 случаев. В марте 2026 г. международные правоохранители ликвидировали два крупнейших ботнета, которые контролировали более 3 млн заражённых устройств по всему миру. Однако уже через месяц количество атак в России выросло на 94% по сравнению с мартом 2026 г., а число заражённых российских устройств увеличилось в 2,6 раза. Сегодня DDoS можно заказать как услугу: существуют платформы, где за определённую сумму клиент получает доступ к ботнету и указывает цель. Это радикально снижает порог входа – для организации мощной атаки больше не нужно быть специалистом по кибербезопасности, достаточно купить эту услугу на рыночных условиях.

Киберпреступники в среднем ежедневно осуществляют около 44 000 ед. DDoS-атак, при этом отдельные организации сообщают о 139 инцидентах в день. Наиболее продолжительная атака длилась 12 388 минут – более восьми суток. Игровая индустрия подвергается примерно 57% всех DDoS-атак, что объясняется высокой чувствительностью игровых сервисов к задержкам в сети. Финансовый сектор и телекоммуникации накапливают по 16,1% атак сетевого уровня, тогда как на электронную коммерцию приходится 22% активности на прикладном уровне. Государственные сервисы также являются значимой целью – на них приходится 38,8% глобальных атак.[2]

Для пользователей, ставших целью целенаправленной DDoS-атаки (что характерно для стримеров, онлайн-геймеров и публичных лиц), стандартными рекомендациями являются смена IP-адреса через провайдера и использование сервисов с встроенной защитой от DDoS. В случае обнаружения признаков участия устройства в ботнете (аномального сетевого трафика, замедления работы интернета, необъяснимого расхода трафика) пользователю следует обратиться к провайдеру и, в наиболее сложных случаях – в национальный центр реагирования на компьютерные инциденты (НКЦКИ – ГосСОПКА), который был создан в 2013 г., активно предотвращает атаки на ресурсы и помогает оперативной работе провайдеров.

Однако, технические рекомендации ухода от DDoS-атаки полезны в том случае, если речь идет о конечных пользователях, а в работе провайдера необходима твердая теоретическая база, которая даст возможность организовать инженерную и техническую работу (организация протокола, маршрутизации, оценка модели угрозы). Именно понимание того, что в ходе атаки стороны делятся на самостоятельных игроков, каждый из которых защищает свои интересы, но при этом они могут для достижения эффекта действовать кооперативно, говорит о возможности выработки стратегии противостояния DDoS-атаки на основе теории игр.

---

[1]За первые шесть месяцев 2026 года общая длительность DDoS-атак практически вышла на уровень всего 2025 года // RUБЕЖ. – 16.07.2026. – URL: https://ru-bezh.ru/kompanii-i-ryinki/news/26/07/16/za-pervye-shest-mesyatsev-2026-goda-obshchaya-dlitelnost-ddos-at?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fdzen.ru%2Fnews%2Fsearch

[2]DDoS-атаки по типам и отраслям – Q1 2026 // Компания «Гарда». – URL: https://garda.ai/blog/analytics/ddos-ataki-po-tipam-i-otraslyam-q1-2026

К возможностям данной теории обращались как зарубежные, так и российские исследователи – Котенко И.В. [1], Вахний Т.В. [2], Клименкова А.С [3], Русинова Д.А. [4] и их коллеги.

Рассматривая алгоритм атаки на пользовательское устройство, мы можем увидеть следующую схему взаимодействия участников (рис.1).

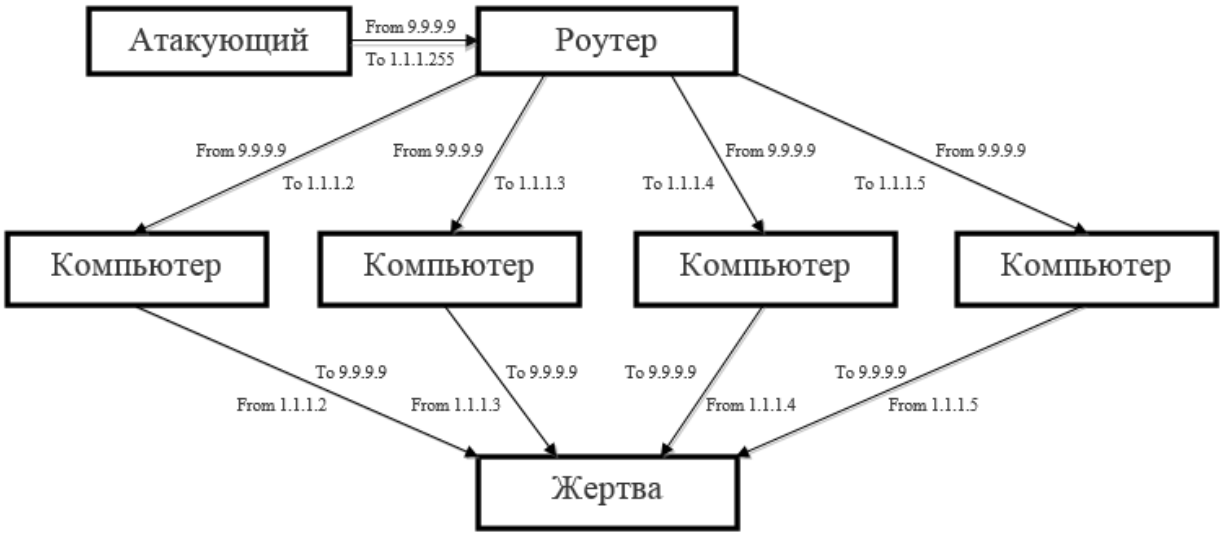


Рис.1 Алгоритм DDoS-атаки

Для поиска оптимального набора средств защиты от различного рода кибератак, включая DDoS-атаки, можно предложить двухстороннюю математическую игру, в которой одним из игроков выступает сама система защиты, а в качестве игрока-противника – возможные кибератаки [1, с. 29].

Роли в данной игре четко распределены. Атакующий (хакер) строит выбор на интенсивности трафика, стараясь нанести ущерб при минимальных затратах на поддержку ботнета и снизив риск своей блокировки. Провайдер, принимая роль защитника, настраивает правила фильтрации запросов: его задача состоит в том, чтобы сделать атаку максимально затратной для злоумышленника, но при этом сохранить доступ к сервису для пользователя, не лишая их возможности пользоваться трафиком. Пользователь задает ориентир нормального поведения системы.

Вознаграждением для атакующего должно быть не обязательно получение прибыли, т.е. это может быть игра с нулевой суммой или ненулевой суммой. Действия, доступные для злоумышленника, – установить количество атакующих потоков из одной машины для выбора количества атакующих узлов [3, с.94].

Игра строится на последовательных решениях каждой из сторон. Оставляем позицию пользователя пассивной, принимая активными участниками провайдера, который оценивает входящий поток и изолирует подозрительную активность, не ограничивая при этом добросовестных клиентов, и атакующего, которому становится нерентабельно наращивать мощность если действия провайдера своевременны. Устойчивое состояние системы достигается тогда, когда ни одной из сторон не выгодно менять выбранную стратегию.

Среди современных компаний ни одна не пренебрегает сохранением устойчивости своих сервисов. Если оценить количество и качество собственных решений, то практически все разработчики встраивают защиту на уровне L3-L4 или L7. Есть и более сложные решения, основанные на амплификации. Российский рынок говорит об удачных решениях в соответствии с ГОСТ или приказами ФСТЭК от следующих компаний: Servicepipe (ООО «Сервиспайп»), Variti (ООО «Варити+»), RED Security (ООО «Ред секьюрити»), Группа компаний «Солар» (АО «СОЛАР СЕКЬЮРИТИ»), Yandex Cloud (ООО «Яндекс.Облако»), АО «Лаборатория Касперского», ООО «СТОРМ СИСТЕМС», ПАО «Ростелеком» и многих других. Все их ПО зарегистрировано в Минцифре, имеет российские лицензии в области связи и защиты информации

Таким образом, использование теории игр для противостояния DDoS-атакам дает шанс современным разработчикам, хостингам и провайдерам использовать игровое преимущество в борьбе за пользователя.

Список использованных источников:

1. Подход к выбору оптимальной стратегии защиты от DDoS-атак на основе применения теории игр / И.В. Котенко, И.Б. Саенко, Ю.И. Синещук, Д.Н. Саратов // Правовая информатика. – 2025. – № 3. – С. 27-36. – DOI 10.24412/1994-1404-2025-3-00-03. – EDN TUHUEN.

2. Вахний, Т.В. Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы / Т.В. Вахний, А.К. Гуц, Н.Ю. Новиков // Математические структуры и моделирование. – 2016. – № 2(38). – С. 103-115. – EDN WDEGNB.

3. Клименкова, А.С. Приложение, реализующее систему защиты Syncookied от DDoS-атак с использованием элементов теории игр / А.С. Клименкова // Математические структуры и моделирование. – 2023. – № 1(65). – С. 86-107. – DOI 10.24147/2222-8772.2023.1.86-107. – EDN DZSXEW.