

Межоператорский бизнес в России в период массовых DDoS-атак

Юлия Цветкова
Екатерина Глебова

Аннотация

В статье рассмотрены виды DDoS-атак, «яркие» примеры взломов сетей операторов на территории РФ. Большое внимание уделено технологиям защиты от DDoS-атак. Рассмотрен рынок России и аномальный рост компаний, которые предлагают решения по защите от DDoS-атак. Также авторы показывают, как операторы связи адаптируются под новые реальности, и демонстрируют дальнейшие перспективы развития и обеспечения безопасности работы сетей связи.



Ключевые слова:

DDoS-атака, распределённые атаки (ботнет), IoT-устройство, сервер, фильтрация трафика.

1. Введение. Новая реальность цифровой экономики

Современный мир, в котором мы живём, неуклонно меняется на протяжении нескольких последних десятилетий, и эти изменения продолжают по сей день. Нет сомнения в том, что одним из ключевых драйверов этих изменений является «цифровая революция». Благодаря цифровым технологиям государства могут повысить свою конкурентоспособность и способствовать экономическому росту за счёт расширения использования этих технологий. Современный межоператорский бизнес — это кровеносная система глобального Интернета, а, следовательно, и развития цифровой экономики. Обмен трафиком (IP-транзит, пиринг) между операторами связи, хостинг-провайдерами и крупными клиентами обеспечивает беспрепятственную работу всего онлайн-пространства: от стриминговых сервисов и банковских приложений до корпоративных сетей и государственных услуг [1].

Компьютерные сети, такие как Интернет, являются основой цифровой экономики. Инфраструктура, обеспечивающая цифровые возможности, состоит из основных физических материалов и организационных механизмов, которые поддерживают существование и использование компьютерных сетей и цифровой экономики. В этой связи становится крайне

важным рассмотреть проблемы взаимодействия операторов связи как игроков на рынке межоператорских услуг, обеспечивающих связность и устойчивость глобальной телекоммуникационной инфраструктуры. А одной из угроз устойчивого развития операторов связи стали массовые DDoS-атаки.

За последние годы значительно выросла сложность и мощность кибератак, в частности, распределённых атак (или ботнет). Атаки перестали быть уделом одиночек-хактивистов и превратились в мощное оружие в руках киберпреступников и инструмент геополитической борьбы. Для межоператорского бизнеса это создало принципиально новые вызовы, где вопрос уже не просто в качестве обслуживания (SLA), а в самом выживании и сохранении репутации [2].

Количество DDoS-атак в первом полугодии 2025 года увеличилось на 60% относительно первого полугодия 2024, пишет «Коммерсант». IT-атаки стали сложнее из-за того, что хакеры чаще начали использовать мультивекторные методы.

При этом на полях ПМЭФ-2025 заместитель председателя правления «Сбера» Станислав Кузнецов сообщил, что в 2025 году ущерб российским компаниям от DDoS-атак увеличился в три или даже более раз. Это произошло на фоне снижения за год общего количества атак. Но они стали значительно сложнее, что в итоге вылилось в большие потери. Россий-

ские компании плохо противостоят зловредному воздействию, а такое противостояние требует системного подхода.

В 2023-2024 гг. СМИ писали об атаках в 1-2 Тбит/с, а в 2025 году акцент сместился на длительные и изнуряющие атаки. Фиксируются атаки, длящиеся несколько дней. Интенсивность таких атак волнообразная. В современных реалиях мощность атаки может достигать 750 Гбит/с, а пик скорости — 138 миллионов пакетов в секунду.

В 2025 году межоператорские каналы стали целью для DDoS-атак. Существует несколько причин. Первая — «эффект домино». Атака на одного крупного оператора или ключевую точку обмена трафиком может парализовать работу десятков или сотен downstream-провайдеров и тысяч конечных клиентов. Вторая причина — мощность современных атак. Объёмы DDoS-атак огромны и могут серьёзно повредить сеть. Третья причина — «слепая» фильтрация, если атака направлена на IP-адрес клиента одного провайдера, но проходит через upstream-оператора. Последний может быть вынужден применить грубую фильтрацию всего трафика к этому провайдеру, чтобы спасти свою собственную сеть. Это коллатеральный ущерб, который бьёт по ни в чём не повинным пользователям. Цель злоумышленников — максимальный ущерб и медийный резонанс [1].

DDoS-атаки на телеком-операторов — это одна из самых серьёзных угроз в цифровом мире, поскольку они затрагивают не просто сайты, а критическую инфраструктуру.

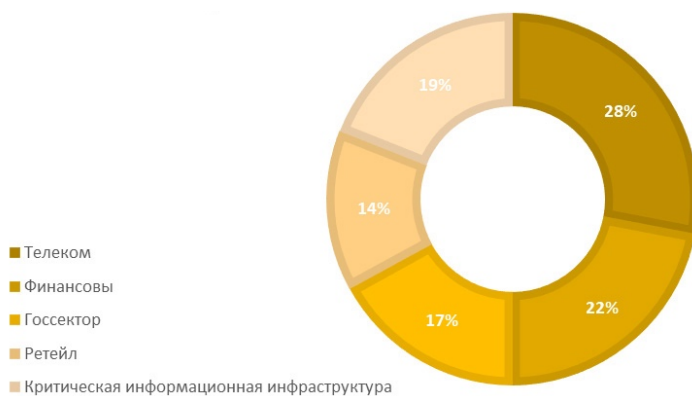


Рис. 1. Основные цели DDoS-атак.

Виды DDoS-атак, последние «яркие» примеры взломов

Существуют различные виды DDoS-атак: по типам трафика, по уровням OSI, по спектру атакуемых объектов. Самые распространённые виды DDoS-атак можно условно разделить на три основные категории:

- уровень приложений;
- уровень протоколов (SYN Flood, ICMP Flood и другие DDoS-атаки уровня протоколов);
- Объёмные (атака UDP Flood в сегменте объёмных DDoS) [3].

Виды DDoS-атак в классификации по уровням OSI

OSI — семиуровневая эталонная модель, описывающая схему взаимодействия сетевых устройств. Модель OSI была разработана еще в 70-х годах и описывала взаимодействие семейства собственных протоколов, которые разрабатывались как главные конкуренты TCP/IP. И хотя особого распространения они так и не получили, модель взаимодействия оказалась настолько удачной, что стала применяться для TCP/IP-протоколов как тогда, так и сейчас. Виды DDoS-атак и защит от них, доступных на каждом из уровней, различны [3].

Классификация уровней:

- 1 уровень. Физический.
- 2 уровень. Канальный.
- 3 уровень. Сетевой.
- 4 уровень. Транспортный.
- 5 уровень. Сеансовый.
- 6 уровень. Представления.
- 7 уровень. Приложений.

С помощью DDoS-атак злоумышленники пытаются полностью прекратить доступ к интернет-ресурсу — отказ в обслуживании. Основной механизм таких атак строится на использовании ботнета — огромной сети заражённых компьютеров, IoT-устройств и серверов, которые злоумышленники контролируют удалённо.

По данным аналитики операторов, предоставляющих защиту от DDoS-атак, за первый квартал 2025 года самыми популярными были атаки типа TCP PSH/ACK Flood, TCP SYN Flood и UDP Flood. Они занимают 76% от общего количества атак.

На операторов связи в основном направляются атаки на инфраструктуру (сетевой и транспортный уровень — L3/L4) и атаки на приложения (прикладной уровень — L7). При атаках L3/L4 уровней целью злоумышленников в телекоме становятся маршрутизаторы (роутеры), межсетевые экраны, базовые станции, каналы связи между городами и странами. Атаки на уровень L7 более изощрённые и сложные для обнаружения. Они имитируют поведение реальных пользователей, но делают это в огромных масштабах. Цели в телекоме: веб-серверы, DNS-серверы, платформы биллинга, сервисы сигнализации.

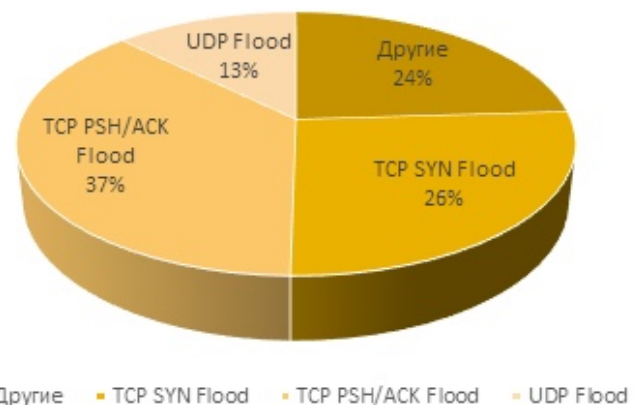


Рис. 2. Типы атак за первый квартал 2025 года.

Статистика дополнительно подтверждает тот факт, что сложные таргетированные атаки от АPT-группировок являются ключевой растущей угрозой, в том числе для телеком-отрасли. Подобные атаки на телеком-сектор влекут за собой и рост числа атак на цепочки поставок с возможностью совершения «атак посредника» (MitM). В результате такой атаки хакеры получают доступ к каналу связи между легитимными сторонами (пользователями, приложениями, сетевыми устройствами и т.д.), что позволяет им просматривать содержимое всех передаваемых ими сообщений, удалять и изменять их. Такие атаки куда сложнее обнаружить как на стороне атакованной жертвы, так и на стороне подрядчика [4].

За текущий год на операторов неоднократно были направлены DDoS-атаки.

28 мая 2025 года специалисты Роскомнадзора сообщили о масштабной DDoS-атаке мощностью 70,07 Гбит/с на московского интернет-провайдера. Из-за DDoS-атаки у части клиентов компании наблюдались проблемы с доступом в сеть.

12 июня 2025 года атаке подвергся интернет-провайдер из Красноярска, в результате чего абоненты из Красноярского края, Хакасии и Иркутской области лишились доступа к Интернету и телевидению. Сетевая и серверная инфраструктура провайдера была выведена из строя киберпреступниками, что привело к масштабному сбою в предоставлении телекоммуникационных услуг. Ситуация оказалась крайне серьёзной, поскольку оператор связи сообщил о возможной утечке персональных данных и попросил клиентов поменять пароли.

30 июля 2025 года масштабной DDoS-атаке на инфраструктуру подвергся крупный петербургский интернет-провайдер.

В качестве особо яркого примера приведём DDoS-атаку в марте 2025 года на одного из крупнейших операторов ШПД на территории РФ. Атака длилась почти пять дней и практически полностью парализовала работу оператора, клиенты оставались без сервисов на весь срок атаки. Разбирая детально данную атаку, мы пришли к выводу, что двумя основными проблемами были ресурсы и компетенции инженеров. Во время атаки на связи были инженеры, не имеющие достаточного опыта в вопросах сети и не имеющие никаких компетенций в защите от DDoS.

Какие основные действия в данном случае могли бы защитить и предотвратить данную ситуацию? Первое: для сайта и мобильного приложения нужна защита WAF, на случай атаки можно включать версию сайта, где сначала выводится captcha, только пройдя которую, можно попасть на сайт. Второе: все структурные сети не должны маршрутизироваться из Интернета. Везде, где можно, необходимо настраивать максимальные правила ACL. В данном примере ГРЧЦ блокировал фактически весь МН-трафик, это убрало атаку на 70%, но остальное нужно было митигировать дополнительными средствами. Тут важно отметить, что на сети должен быть, как минимум, один защищенный апстрим, под защиту которого можно поставить какие-то точечные суперважные сети. По результатам разбора ситуации оказалось, что на сети оператора было несколько взломанных абонентских устройств, откуда, видимо, злоумышленники проводили разведку и следили за принимаемыми контрмерами. Сначала упал сервер L2TP, через который настраивался удалённый доступ к

сети. Видимо, по этой же причине квалифицированные сотрудники не смогли вовремя подключиться к проблеме. И здесь делаем вывод, что обязательно нужны какие-то альтернативные точки входа на чужих IP. Так, нужно отметить, что у атаки была заметная предпосылка — фишинговая атака, т.е. письма с вложением, после открытия и запуска которого в системе устанавливался удалённый доступ к компьютеру. До этого были атаки в Telegram — «сообщения от руководства компании», но это напрямую оператору связать с атакой не удалось. Также в этом примере стоит отметить, что атака была на ту часть сети, которая задевает максимум инфраструктуры. Это говорит о качественной подготовке атаки. Систем предотвращения вторжений (IPS) и обнаружения вторжений (IDS) у оператора не было, а это могло бы сигнализировать о возникновении повышенного внимания к инфраструктуре. В заключение по данному примеру хотим отметить, что в качестве превентивных мер необходимо иметь резервный «чужой Интернет» и «чужие IP-адреса» (/24 достаточно), а возможно, и реализацию полноценной схемы с переводом всех абонентов «на чужой BRAS».

Разобрав виды и примеры атак на операторов, перейдём к видам защиты.

Виды защиты от DDoS-атак, технологии реализации

От DDoS-атак есть множество современных способов защиты. Ниже перечислим основные виды защиты:

1. Фильтрация трафика.
2. Использование CDN (Content Delivery Networks).
3. Web-Application Firewall (WAF).
4. Облачные и гибридные решения Anti-DDoS.
5. Мониторинг и автоматическое реагирование.
6. Ограничение скорости соединений и ресурсов.
7. Резервирование ресурсов и масштабирование.
8. План реагирования на инциденты.

Возрастающее значение приобретают гибридные модели, сочетающие локальную защиту с облачными сервисами. Комбинация сетевого и прикладного уровней защиты обеспечивает комплексную безопасность. Внедрение защитных технологий на уровне интернет-провайдеров и дата-центров значительно повышает надёжность.

Во время DDoS-атаки для оператора крайне важно поддерживать доступность и прохождение «чистого» трафика, пока идёт отражение атаки.

DDoS-атаки несут огромные потери для всех сфер бизнеса и государственных структур. Простой и деградация сервиса ведут к финансовым штрафам и потере доверия со стороны клиентов. Потеря статуса надёжного партнёра может привести к резкому оттоку клиентов.

Для предотвращения DDoS-атак клиент должен заранее позаботиться о своей защите. Успешное отражение

DDoS-атаки позволят сохранить инфраструктуру, клиентов и репутацию. Инвестиции в профессиональную защиту от DDoS-атак — это необходимость, такая же важная, как разработка бизнес-плана.

Выживание в период современных DDoS-атак требует комплексного подхода. Необходимо внедрить системы очистки трафика на границе собственной сети, гибкую маршрутизацию (BGP Flowspec, RTBH), резервирование каналов, постоянный мониторинг, способный мгновенно реагировать на инциденты.

Для противодействия угрозам от DDoS-атак необходима профессиональная митигация. Для защиты своих клиентов компании предлагают услуги защищённого хостинга со встроенными anti-DDoS-решениями. Весь входящий трафик перенаправляется в специальные центры очистки (scrubbing), где происходит его анализ и фильтрация, после чего «чистый» трафик отправляется на сервер клиента. Это позволяет обеспечить целевую доступность сервиса для пользователей даже во время атаки.

Российский рынок «предложений по защите»

Массовые DDoS-атаки из эпизодических превратились в суровую ежедневную реальность. Борьба с DDoS-атаками — это непрерывная «гонка». Операторам приходится постоянно инвестировать в сложные, многоуровневые системы защиты, чтобы обеспечивать надёжную связь для своих клиентов.

Стоит отметить очень важный момент, что массовые DDoS-атаки создали новый рынок услуг. Вследствие высокой геополитической напряжённости и активности как киберпреступников, так и политически мотивированных хактивистских групп, рынок услуг по защите от DDoS-атак развивается очень быстро. Российский сегмент интернета (Рунет) стал постоянной мишенью для крупномасштабных и сложных атак. Российским операторам и компаниям приходится самостоятельно искать способы для борьбы с кибератаками. Такое положение способствует быстрому и уникальному развитию рынка по защите от DDoS-атак. В России спрос на услуги защиты от DDoS-атак продолжает стабильно расти. Запрос исходит не только от крупного бизнеса (финансы, госсектор, телеком, крупный ретейл), но и всё чаще от среднего и даже малого бизнеса, чья онлайн-активность критически важна (интернет-магазины, образовательные платформы, агрегаторы услуг).

Крупными игроками рынка защиты от DDoS-атак являются ведущие компании, предлагающие комплексные технические решения и сервисы для различных масштабов бизнеса. Игроки российского рынка, занимающиеся защитой от DDoS-атак, отличаются масштабируемостью, продвинутыми технологиями фильтрации трафика, использованием ИИ и машинного обучения, а также интеграцией нескольких уровней защиты. Они обеспечивают надёжную оборону для крупного и среднего бизнесов, государственных структур, а также интернет-площадок.

Производители ПАКов (программно-аппаратный комплекс): разрабатывают и поставляют специализированное аппаратное и программное обеспечение для обнаружения и отражения DDoS-атак. Их продукты обычно предназначены для развёртывания в периметре заказчика (или провайдеров услуг).

Телеком-провайдеры: предоставляют услуги защиты от DDoS-атак на уровне своей инфраструктуры и сетей. Они предоставляют своим клиентам услуги «чистого» трафика, фильтрацию DDoS-трафика и прокси-серверы. Такие услуги обычно предлагаются в виде абонентских платежей или по запросу клиентов.

Сервис-провайдеры: предлагают облачные услуги защиты от DDoS-атак. Они могут действовать в качестве промежуточного звена между клиентами и их веб-приложениями, обрабатывая весь трафик и фильтруя его, прежде чем он достигнет клиентской инфраструктуры. Эти сервисы обычно предоставляются по модели подписки и могут включать в себя дополнительные функции, такие как CDN (Content Delivery Network) и функции оптимизации производительности.

Стоит отметить важное изменение на рынке межоператорского бизнеса: в новых реалиях крупные игроки рынка теперь

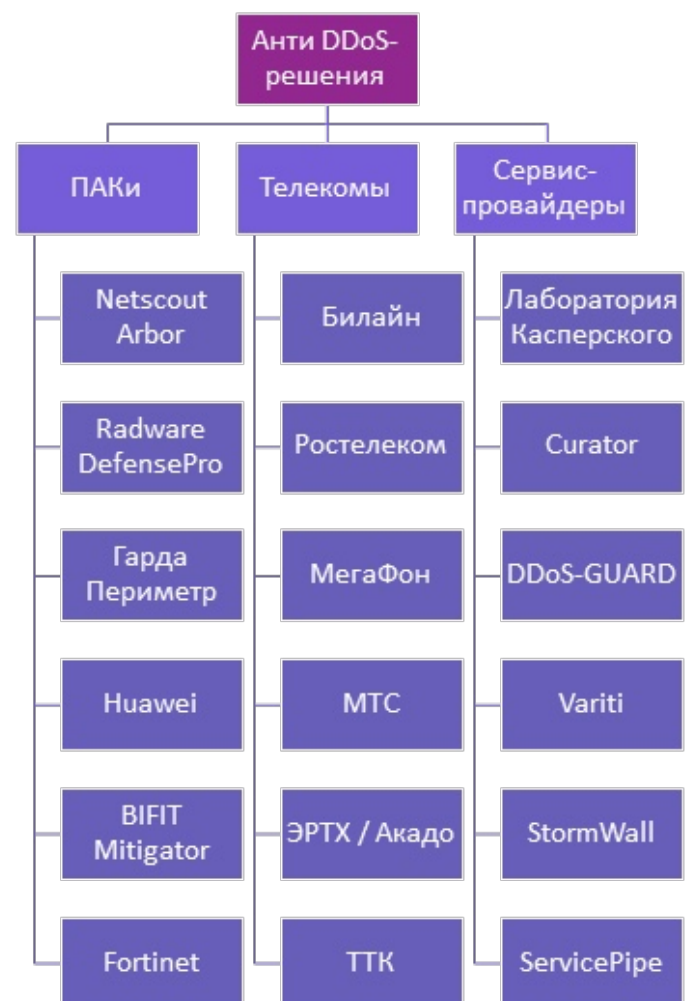


Рис. 3. Основные участники российского рынка защиты от DDoS-атак.

предлагают не просто IP-транзит, а «защищённый IP-транзит» — услугу, где трафик по умолчанию проходит через систему очистки. Кроме того, операторы могут предлагать услуги DDoS-защиты «в облаке» для своих партнёров, у которых нет ресурсов для развёртывания собственных дорогостоящих систем. Тут в качестве примера приведём ПАО «ВымпелКом»,

одного из крупнейших игроков этого рынка, который реализовал сразу несколько комплексных решений IP-транзит плюс защита от DDoS-атак и в 2025 году успешно защитил нескольких своих клиентов-операторов от мощнейших DDoS-атак

Успех теперь определяется не только ценой за гигабит или

| Оператор (Россия) | Публично упомянутые решения / партнёры (вендоры, сервисы) | Тип развёртывания / модель |
|--|---|--|
| «Билайн» («ВымпелКом»), включая beeline cloud | Radware (исторически запуск сервиса с Radware), собственные DDoS-услуги Beeline Cloud; NetFlow-продукт на базе центра очистки; партнёрство с Kaspersky. | Комбинация: on-prem (вендорское hw/sw) + облачные услуги для клиентов; фильтрация в сети оператора и центры очистки. |
| «Ростелеком» (вкл. «Солар») | Curator Labs, собственные решения Anti-DDoS («Ростелеком-Солар») на базе «Периметр-Гарда». | Гибрид: внутренняя защита + внешние инструменты/партнёрства; фильтрация в сети оператора и центры очистки. |
| МТС / Red Security / MWS | Curator Labs (партнёрство: CloudMTS сервис на базе Curator). | Облачный скраббинг / MSSP интеграция (Cloud-service). |
| «МегаФон» | Сервис на базе «Периметр-Гарда». | Операторский «cloud + network» фильтр; уровень защиты каналов и приложений (операторская услуга). |
| ТТК («ТрансТелеком») | Услуга DDoS Free на базе «Периметр-Гарда» и решения DDoS-Guard Protection. | Операторский центр очистки (scrubbing centre) + мониторинг 24/7. |
| «ЭР-Телеком» / «Дом.ру» (региональные операторы) | Операторские Anti-DDoS-сервисы; часто используют решения Servicepipe и Ddos-Guard (партнёры в регионах варьируются). | On-prem + облачные центры очистки; услуга для B2B/госзаказчиков. |
| Т2 / (в регионах и дочерних структурах) | Предлагает Anti-DDoS-услуги на базе продуктов «Ростелекома». | Операторская услуга (обычно BGP-redirect → скраббинг). |
| G-Core Labs (не оператор, но крупный провайдер скраббинга) | Собственная сеть скраббинга (global DDoS protection), TMS (threat mitigation system). | Облачный/глобальный scrubbing (Anycast, многотераваттная ёмкость - указывают в маркетинге). |
| Curator Labs (MSSP / scrubbing provider) | Собственная распределённая сеть фильтрации, интеграции с операторами и облаками (Yandex.Cloud, CloudMTS и пр.). | Anycast BGP, filtering points (скраб-узлы) — облачный скраббинг + интеграции. |
| Прочие российские вендоры/MSSP (Kaspersky, StormWall, DDOS-GUARD и др.) | Kaspersky DDoS Protection, StormWall, DDoS-Guard, MWS, K2.Cloud — коммерческие продукты/услуги. | Обычно облачный скраббинг, WAF, антиботы, локальные appliances в дата-центрах. |
| Аппаратные вендоры, часто встречающиеся в телеком-решениях (общая категория) | Radware (DefensePro), Arbor / Netscout (Peakflow / APS), Cisco (IOS/Firepower + FlowSpec), Huawei. | On-prem appliances, flow-based detectors, FlowSpec/BGP-redirect интеграции, hybrid cloud. |

Рис. 4. Конкурентный анализ B2O-решений «Анти-DDoS».

шириной канала, но и способностью гарантировать доставку трафика в самых неблагоприятных условиях. Оператор, который может продемонстрировать партнёрам и клиентам отработанные механизмы противодействия, проактивный мониторинг и прозрачность коммуникации, получает ключевое конкурентное преимущество в эпоху цифрового шторма.

Выживает не самый большой, а самый гибкий и подготовленный. В современной интернет-экосистеме безопасность — это не затраты, это фундамент для доверия и роста. Разберём пример, на котором покажем, почему защита от DDoS-атак не может стоить дёшево. На сети телеком-провайдера с нормой в 300 Гбит/с

легитимного трафика начинается атака мощностью в 200 Гбит/с, распределённая по восьми тысячам IP-адресов. Чтобы от неё защититься, ёмкость очистителей оператора должна суммарно покрывать объёмы и легитимного, и вредоносного трафика на большой сетевой сегмент, то есть в данном случае составлять не менее 500 Гбит/с. Таким образом, для эффективной защиты система фильтрации должна иметь запас по объёму для качественной работы. Этот запас ёмкости должен быть постоянен, а значит, и цена сразу вырастает в разы. Причём этот запас должен быть рассчитан на каждого клиента, так как предугадать, какие клиенты станут жертвами DDoS-атак, невозможно.

Перспективы развития рынка защиты от DDoS-атак

Развитие интеллектуальных систем и интенсивный рост киберугроз стимулируют развитие систем на базе искусственного интеллекта (ИИ) и машинного обучения, которые способны выявлять аномалии и новые типы атак в режиме реального времени. В будущем алгоритмы ИИ будут всё глубже и глубже внедряться в системы защиты, обеспечивая быструю и точную фильтрацию вредоносного трафика.

Мы предполагаем, что в будущем защита будет состоять из нескольких этапов: сначала будет защищаться сетевой уровень (фильтрация и стабилизация трафика), далее — прикладной уровень, где защищаются API и веб-приложения, и в завершение будут специализированные механизмы защиты на базе ИИ от ботов и массированных сканирующих атак. Такая модель позволит гибко адаптироваться к особенностям инфраструктуры.

Скорее всего, злоумышленники будут совершенствовать свои атаки, и, как следствие, атаки станут мощнее, скоростные пики выше, а длительность дольше.

Внедрение автоматизации в системы реагирования позволит минимизировать время простоя и оперативно реагировать на новые векторы атак, включая использование ИИ как в атакующих инструментах, так и в средствах защитной аналитики.

В нашей текущей современности мы наблюдаем рост количества IoT-устройств и их связей, которые могут формировать новые ботнеты, состоящие из бытовых и промышленных устройств. Для мониторинга и фильтрации трафика, с учётом особенностей таких устройств, необходима разработка новых подходов.

Рынок по защите от DDoS-атак продолжит свой быстрый рост. Будут разрабатываться новые системы и алгоритмы, а также широкое применение получит ИИ. Продолжат совершенствоваться комплексные подходы защиты. В перспективе возможно создание единой платформы безопасности.

Возможно, защита от DDoS-атак будет связана с анализом на уровне ИИ, многоуровневой защитой, автоматизацией и интеграцией современных технологий, что позволит своевременно и эффективно противостоять вновь возникающим угрозам в условиях быстрого роста и развития DDoS-атак. ■

Список литературы:

- [1] «Кибербезопасность и защита информации в интернет-сетях» — Михаил Калугин.
- [2] Ежегодный отчет StormWall о DDoS-угрозах. <https://stormwall.pro/>
- [3] Что такое DDoS атака. Настройка эффективной защиты от DDoS атак на сервер. Хостинг RigWEB. <https://rigweb.ru/>
- [4] Тренды кибератак на промышленность и телеком в 2025 году. <https://rt-solar.ru/>

Об авторах

Цветкова Юлия Валерьевна, к.т.н., ПАО «ВымпелКом», Москва
Глебова Екатерина Сергеевна, ПАО «ВымпелКом», Москва

