

5 МИФОВ, КОТОРЫЕ ДЕЛАЮТ ЗАЩИТУ ОТ DDoS НЕЭФФЕКТИВНОЙ

Гайд для тех, кто хочет построить эффективную защиту

Веб-ресурс — критически важный элемент цифровой стратегии компании

- Пользователи хотят, чтобы веб-ресурс работал без сбоев 24/7
- Каждая минута простоя веб-ресурса — потеря денег и репутации
- Веб-ресурс — объект целенаправленных кибератак

Многие списали DDoS со счетов, но он продолжает эволюционировать. Злоумышленники перешли от лобовых ударов к точечным атакам бизнес-логики.

Как построить или адаптировать защиту от DDoS с учетом новых вводных?

Я Ник из суппорта NGENIX. И я собрал для вас 5 мифов, из-за которых снижается устойчивость веб-ресурсов к DDoS-атакам.



МИФ № 1

« У НАС ON-PREM. ЭТО ЛУЧШЕЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ОТ DDoS »

В 2026 у многих компаний уже есть защита от DDoS-атак. Один из привычных подходов — on-prem-решения. Это системы защиты, развёрнутые в инфраструктуре конкретной организации (на собственных серверах и оборудовании).

Рассчитывать на то, что текущих мощностей on-prem-решения будет достаточно для защиты в 2026, крайне рискованно. Мощность DDoS-атак растёт экспоненциально: в 2025 были зафиксированы атаки с нагрузкой 10+ Тбит/с.

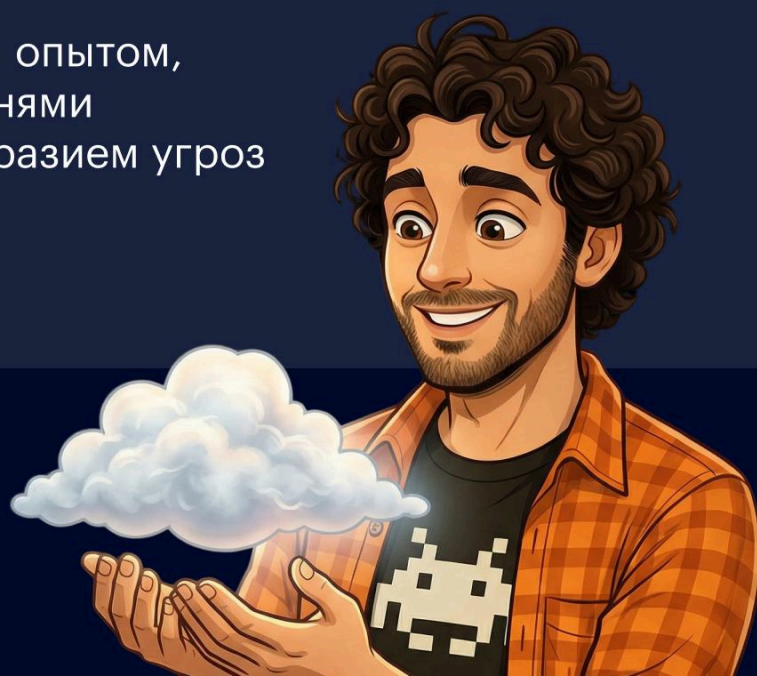
Использование on-prem становится неэффективным и крайне дорогим, так как невозможно эффективно масштабировать систему для отражения объёмных DDoS: физическое оборудование имеет ограничения по пропускной способности и вычислительным ресурсам.

При этом внедрение и обслуживание своего оборудования требует больших инвестиций на покупку железа, найм специалистов для поддержки и мониторинга системы.



Совет: Присмотритесь к облачным решениям для защиты от DDoS-атак.

- 1** У облачных провайдеров защиты есть эластичная инфраструктура, которая автоматически масштабируется под пики нагрузки и демпфирует атаки, распределяя трафик по множеству узлов в разных географических точках.
- 2** Использование облачных решений экономически выгоднее, чем построение и поддержка собственной on-prem-системы. Не нужно тратить средства на закупку и обновление оборудования, на обучение и содержание штата специалистов. Также можно избежать расходов на обработку нелегитимного трафика — провайдер фильтрует его до попадания в вашу сеть, поэтому вы не платите за нелегитимный входящий трафик, он не тарифицируется.
- 3** Команда провайдера обладает разносторонним опытом, который накапливается благодаря работе с сотнями различных кейсов. С таким объёмом и разнообразием угроз отдельная компания обычно не сталкивается.



МИФ № 2

« МЫ ПРОПУСКАЕМ ВЕСЬ ТРАФИК ЧЕРЕЗ WAF. ЭТОГО ХВАТИТ ДЛЯ ЗАЩИТЫ ОТ DDoS »

Некоторые считают, что WAF — это щит, который отражает все виды атак и уязвимостей, в том числе идеально справляется с DDoS-атаками. В реальности, анализ входящего трафика на уровне WAF — слишком ресурсоёмкая задача.

Когда веб-ресурс находится под шквалом «мусорных» запросов, инфраструктура WAF может не справиться с большим объёмом трафика. Проверка даже самого простого запроса происходит с использованием всего набора инструментов и фильтров: сигнатуры, поведенческий анализ и другие.

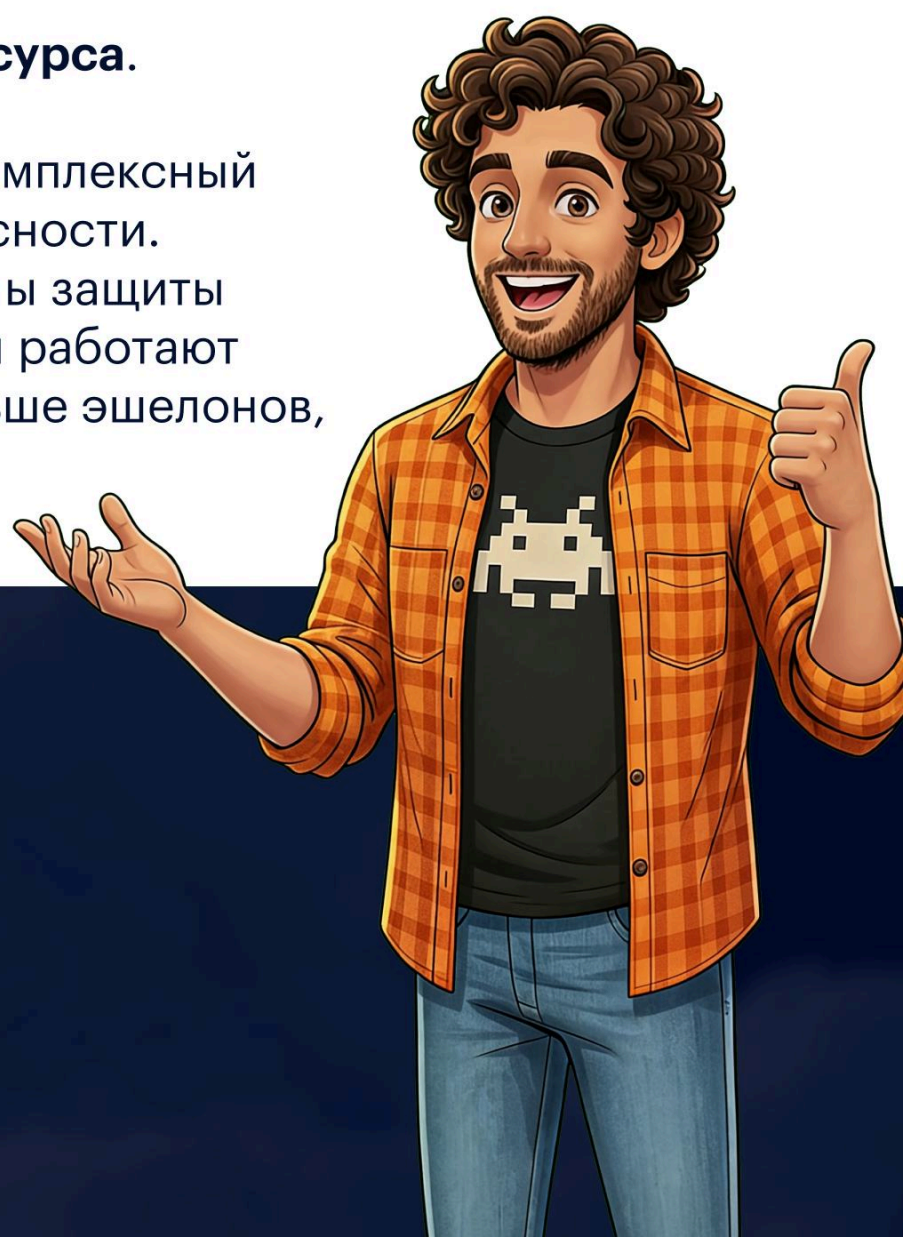
В случае объёмной атаки попытка защититься от DDoS с помощью WAF, скорее всего, наоборот — сделает сайт недоступным ещё быстрее.

Также стоит учитывать, что WAF — это инструмент защиты на L7. А большинство объёмных атак происходит на L3/L4. WAF не будет полезен при таком сценарии.

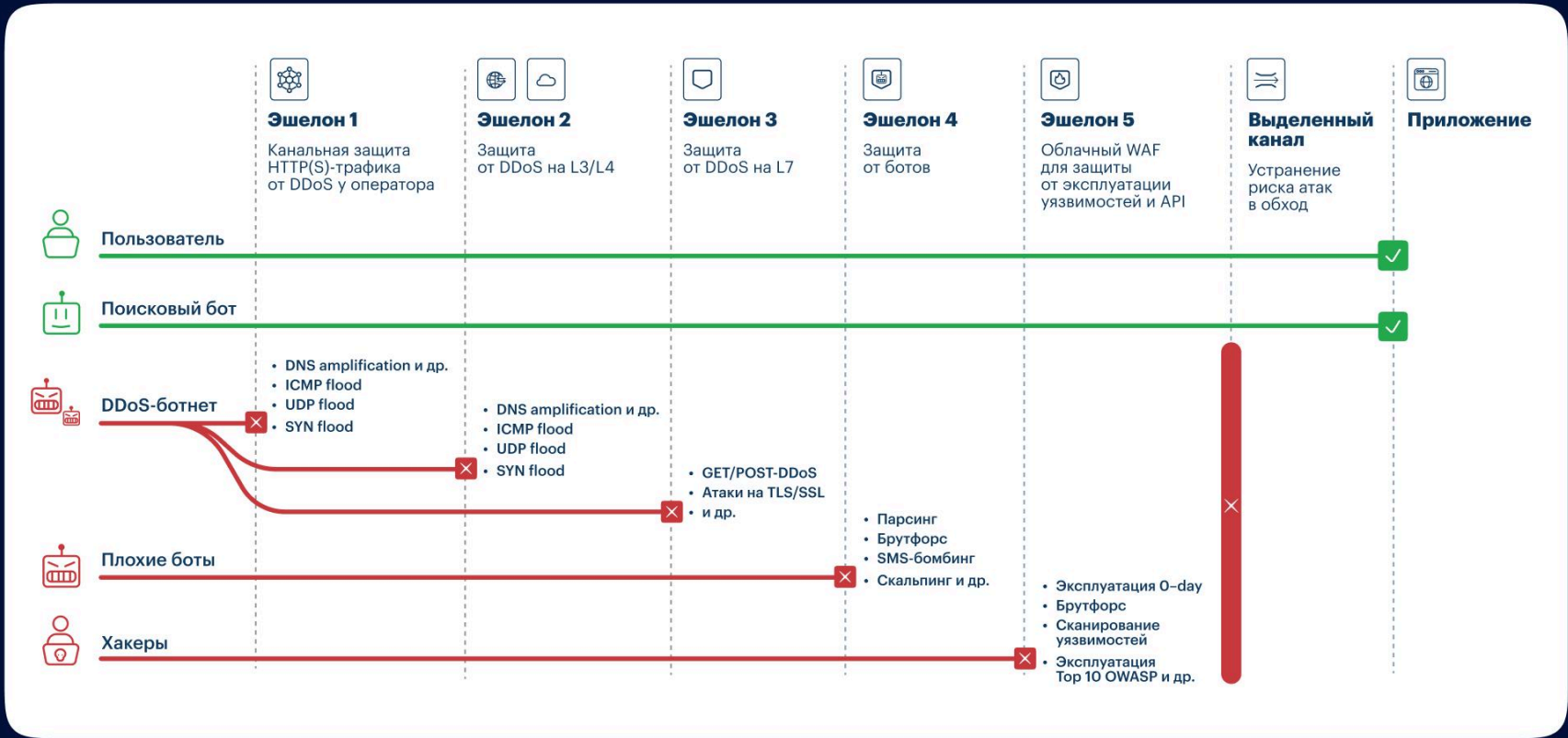


Совет: Рекомендую выстраивать эшелонированную защиту веб-ресурса.

Эшелонированная защита — это комплексный подход к обеспечению веб-безопасности. Он строится на разделении системы защиты на несколько эшелонов. На каждом работают разные средства защиты. Чем больше эшелонов, тем выше уровень защищенности.



Какой может быть эшелонированная защита (показываем на примере NGENIX):



- **Эшелон 1** — канальная защита HTTP(S)-трафика на L3/L4, которую обеспечивают операторы и хостеры. Отражение масштабных DDoS-атак на каналы (UDP-флуд, ICMP Flood и SYN Flood).
- **Эшелон 2** — защита от DDoS-атак на L3/L4 путем маскировки IP-адреса. NGENIX выполняет функцию реверс-прокси: IP-адрес инфраструктуры заказчика изменяется на IP-адрес платформы. Если злоумышленник не знает реальный IP-адрес цели атаки, он будет атаковать серверы NGENIX.
- **Эшелон 3** — защита от DDoS-атак на L7. Система анализирует HTTP(S)-трафик, распознаёт аномалии и вредоносные запросы и применяет гибкие меры защиты — от незамедлительной блокировки до дополнительных проверок.
- **Эшелон 4** — защита от ботов, которые могут имитировать поведение реальных пользователей, негативно влиять на нагрузку веб-приложений и повышать затраты. Фильтрация трафика по репутации, эвристикам, поведенческому, статистическому, сигнатурному анализу позволяет защищать сайт от парсинга, брутфорса, скальпинга, SMS-бомбинга и других бот-атак.
- **Эшелон 5** — облачный WAF глубоко анализирует запросы, защищая приложение от SQL-инъекций, межсайтового скриптинга, уязвимостей из OWASP Top-10 и других угроз. Этот эшелон нужен для отражения особо сложных атак. Он усиливает защиту и минимизирует риски взлома. Нагрузка на WAF снижена, так как примитивные атаки отражаются на предыдущих эшелонах.

Чтобы эшелонированная защита работала ещё эффективнее, мы предлагаем подключение к платформе NGENIX по выделенному каналу для предотвращения риска атак в обход защиты. Подробнее об этой угрозе можно узнать [здесь](#).

МИФ № 3

« ЗАЩИТЫ НА L3/L4 ХВАТИТ. ОСТАЛЬНОЕ — ТРАТА ДЕНЕГ »

Многие считают, что защиты от DDoS на L3/L4 достаточно. Но сейчас атаки всё чаще нацелены не на выведение веб-ресурса из строя, а на «обесточивание» его ключевых функций бизнес-логики: авторизации, поиска, API, платёжных шлюзов.

По нашим данным, 60% атак направлены на уязвимости бизнес-логики приложений. Это значит, что даже идеальная защита на L3/L4 не спасёт, если веб-приложением нельзя воспользоваться по назначению.

Например, может быть атака на функцию «сброса пароля» (OTP-flood). Злоумышленник через API дергает восстановление пароля для тысячи пользователей, забивает этим SMS или почту. Спам-фильтры тут бессильны. Нужна защита, которая понимает контекст запроса и может зарейтмитить именно эту операцию, не трогая остальной функционал.



Совет: **Выстраивайте защиту не только на сетевом и транспортном уровне, но и на уровне приложений.** Выбирайте провайдера, который может дать комплексную защиту на L3, L4 и L7, а также защиту API и защиту от нежелательных ботов.



МИФ № 4

DDOS — В ПРОШЛОМ, ЕГО СТАЛО МАЛО. НАМ ХВАТИТ БАЗОВОЙ ЗАЩИТЫ

Ещё одно заблуждение. Число DDoS-атак может снижаться, но их эффективность растёт. Злоумышленники перешли от лобовых ударов к изощрённым методикам.

В числе трендов:

Ковровые бомбардировки

Злоумышленники распределяют вредоносный трафик по тысячам IP-адресов в рамках одной сети или подсети. На каждый адрес приходится относительно небольшой объём трафика, который может не превышать пороги срабатывания системы защиты. Одновременная нагрузка на множество адресов приводит к перегрузке инфраструктуры.

Burst-атаки

Злоумышленники генерируют короткие всплески трафика, каждый значительно превышает обычную нагрузку на систему. Всплески повторяются с короткими интервалами и не дают инфраструктуре восстановиться после предыдущего удара. Классические Anti-DDoS-системы имеют инерцию: им нужно время, чтобы выявить аномалию. Из-за этого возникают микролаги, которые ухудшают пользовательский опыт и перегружают ИБ-команду частыми срабатываниями.



Совет: Сегодня базовой защиты от DDoS недостаточно: она опирается на поиск статистических аномалий, а современные атаки их не создают. **Для эффективной защиты нужен микс решений.**

- 1 Классические методы (фильтрация по IP, rate limiting и другие) нужны для отражения простых атак. Эти инструменты остаются актуальными для базового уровня защиты: они экономичны, просты в настройке и не создают лишней нагрузки на инфраструктуру.
- 2 Поведенческий анализ нужен для выявления подозрительных паттернов даже при отсутствии статистических аномалий. Система отслеживает не абсолютные показатели, а отклонения в поведении пользователей: например, неестественную скорость запросов или повторяющиеся последовательности действий.
- 3 Челленджи (CAPTCHA, JS-проверки, проверка TLS-отпечатка и другие) нужны для блокировки ботов с первого запроса. Такие механизмы требуют от клиента выполнения дополнительного действия или подтверждения легитимности соединения. Это практически не влияет на обычных пользователей, но эффективно блокирует автоматизированные атаки.

МИФ № 5

« МЫ ДЕЛЕГИРОВАЛИ ЗАЩИТУ ПРОВАЙДЕРУ. ОТ НАС БОЛЬШЕ НИЧЕГО НЕ НУЖНО »

Часто компания заключает договор с провайдером защиты и полностью устраняется от вопросов безопасности, считая, что подрядчик сам обнаружит угрозы, примет решение по их отражению, будет обновлять защиту под новые риски.

Но аутсорсинг киберзащиты — это не «волшебная таблетка».

Отсутствие диалога и обратной связи снижает эффективность защиты. Если компания не делится данными о подозрительных инцидентах или изменениях в архитектуре, подрядчик не сможет адаптировать правила фильтрации или сценарии реагирования.

Например, если не рассказать провайдеру о новом API-эндпоинте, он не настроит для него правила защиты. Злоумышленники могут использовать такой эндпоинт как точку входа, несмотря на высокий уровень защиты остальных компонентов веб-ресурса.



Совет: Выстраивайте партнёрство с подрядчиком, а не просто делегируйте задачу.

Настройте регулярный обмен информацией:

- передавайте подрядчику данные о планируемых релизах, пиковых нагрузках, новых сервисах — это поможет избежать ложных срабатываний;
- запрашивайте отчёты о выявленных угрозах и методах их отражения — это даст инсайты для внутренней ИБ-стратегии;
- оперативно сообщайте о подозрительных сигналах (странные запросы, необычные логи, попытки доступа);
- обсуждайте и анализируйте интересные кейсы.

Мы, например, получаем от заказчиков продуктовые инсайты, которые помогают развивать и улучшать сервисы защиты.



ЧЕК-ЛИСТ ЭФФЕКТИВНОЙ ЗАЩИТЫ ОТ DDoS В 2026 ГОДУ

Оцените готовность вашей инфраструктуры к отражению DDoS-атак. Отметьте, какие меры защиты уже внедрены, а какие требуют внимания.

- ☐ Есть защита от DDoS-атак на L3/L4
- ☐ Есть защита от DDoS-атак на L7
- ☐ Настроен rate limiting на уровне отдельных эндпоинтов (например, авторизации, сброса пароля, поиска, оплаты)
- ☐ Проведена инвентаризация API: выявлены и закрыты «теневые» или устаревшие интерфейсы, которые могут стать точкой входа
- ☐ Реализована защита от злоупотребления бизнес-логикой веб-ресурса (например, от скальпинга или брутфорса)
- ☐ WAF интегрирован в состав эшелонированной защиты: через него не идет весь трафик
- ☐ Есть возможность экстренного масштабирования ресурсов при объёмной атаке
- ☐ Настроены механизмы распределения трафика по глобальным точкам фильтрации
- ☐ Внедрены антибот-решения с поведенческим анализом

ОБНАРУЖИЛИ ПРОБЕЛЫ?

Не ждите, пока злоумышленники воспользуются ими!

Напишите нам: sales@ngenix.net

Мы поможем выстроить эффективную защиту от DDoS-атак:

- подскажем оптимальные решения для незакрытых пунктов,
- подберём инструменты защиты под ваш бюджет и ваши задачи.

 Узнать больше о наших решениях для защиты веб-ресурса можно на ngenix.net

