

Отчет о веб-угрозах за III кв 2026 года

По данным PT AF Cloud

Главные выводы

Общий поток событий безопасности во II–III кварталах 2026 года увеличился на 12%, однако в отдельных категориях динамика оказалась кратно выше:

ИИ-маркеры: +65% за III квартал. Автоматизированные клиенты и ИИ-агенты перестают быть просто сборщиками контента и все чаще генерируют вредоносные запросы к приложениям.

React/Next.js: +104% за III квартал. Спустя девять месяцев после раскрытия React2Shell интерес к уязвимости по-прежнему высокий.

Общая картина по событиям



Нормализованный индекс темпа роста: общий поток=1,0
Индекс = темп роста категории/ темп роста общего потока

Рис. 1

Картина угроз развивается неравномерно: новости вокруг критически опасной уязвимости исчезают из медиа за считанные дни, но автоматизированные сканеры продолжают методично проверять инфраструктуру месяцами. Поэтому для защиты от актуальных угроз важно отслеживать не только количество событий, но и то, как меняются характер и инструменты атак.

В основе исследования — обезличенная статистика PT Application Firewall Cloud (PT AF Cloud) за 3 квартал 2026 года, отражающая реальные попытки обхода правил безопасности на защищаемых ресурсах клиентов.

ИИ-клиенты заметнее в событиях безопасности

В III квартале число событий с явными ИИ-маркерами **выросло на 65%** по сравнению со II кварталом. Август стал пиковым месяцем: после июльского минимума показатель вырос в 3,8 раза. В сентябре он снизился, но оставался почти втрое выше июльского уровня.

На графике отмечены публичные релизы:

- Gemini 3.5 Flash в мае
- GPT-5.6 Sol в июне
- GPT-6 Astra в сентябре

Августовский пик произошел до выхода Astra. Возможная причина снижения в июле — злоумышленникам требуется время, чтобы освоить новые модели и начать использовать их. Сентябрьский спад закономерен: первая волна экспериментов схлынула, а релиз GPT-6 Astra состоялся только в начале месяца.

В следующем периоде станет понятнее, приведет ли выход GPT-6 Astra к новой волне запросов и как быстро новые модели начнут использоваться в атаках.

Динамика событий с ИИ-маркерами на фоне крупных релизов моделей

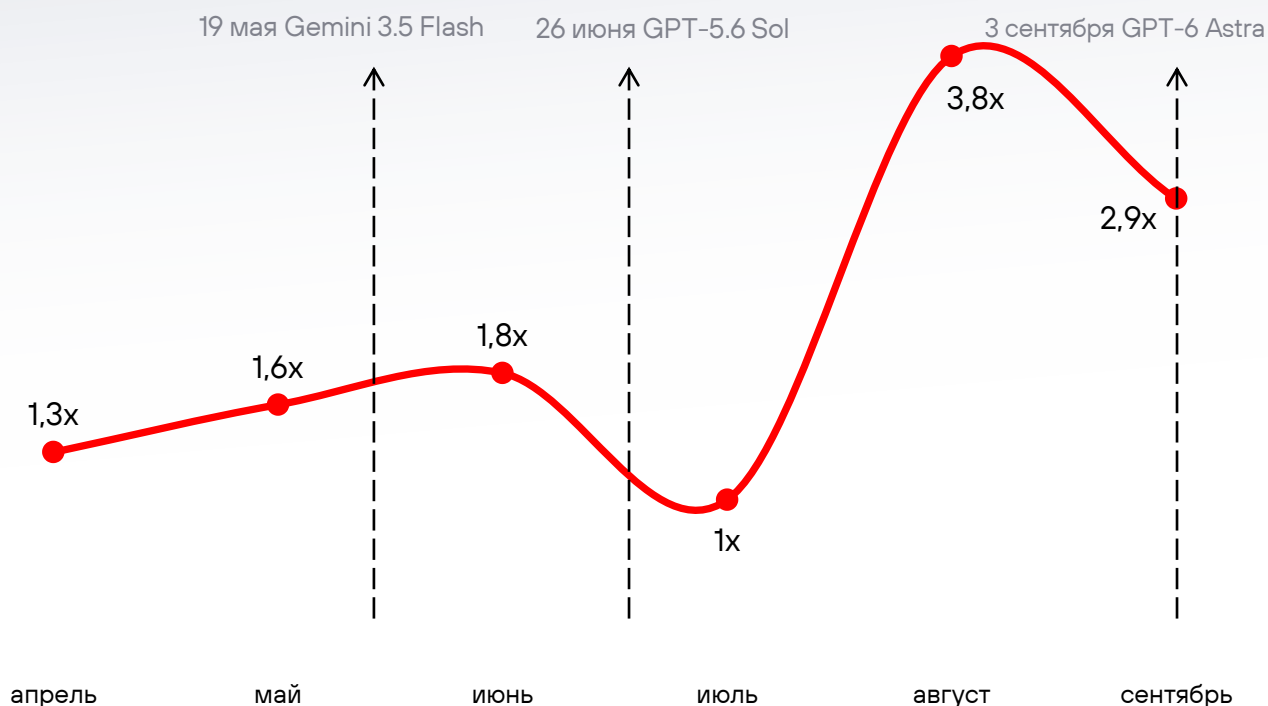


Рис.2

ИИ-маркеры позволяют видеть, как меняется состав автоматизированных обращений и как часто они вызывают события безопасности.

Автоматизация требует отдельной политики доступа

Среди явно автоматизированных событий доля ИИ-маркеров **увеличилась с 5,6% до 6,8%**. В выборку включены ИИ-клиенты, боты, инструменты ИБ и мониторинга.

Полезным роботам можно открыть нужные ресурсы, а нежелательные массовые обращения ограничивать: универсальное правило для всех автоматизированных клиентов быстро перестает работать.

ИИ-маркеры в наблюдаемом автоматизированном потоке

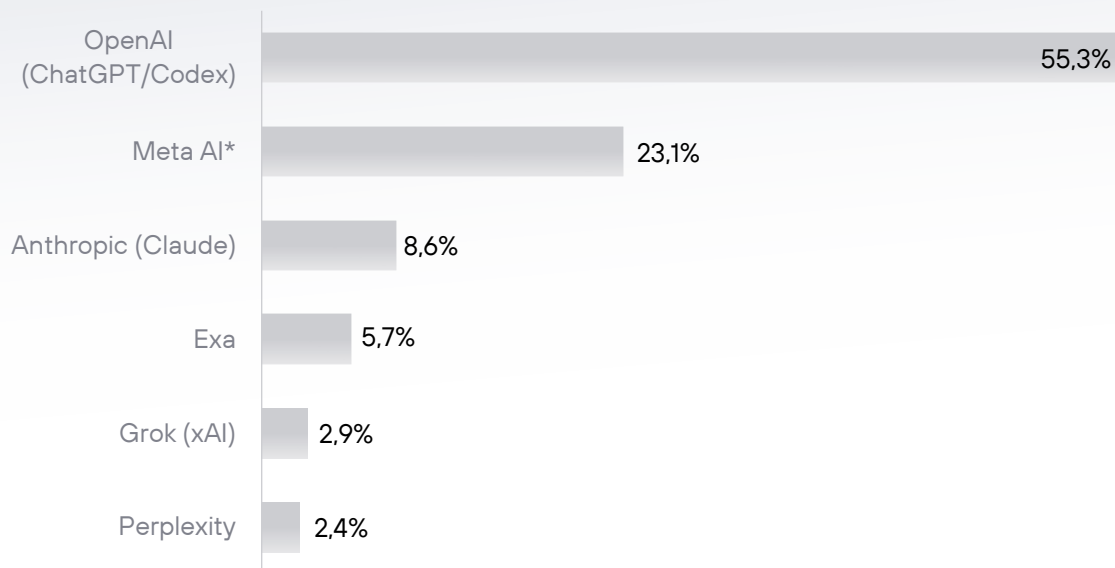


Учтены ИИ-клиенты, боты, инструменты ИБ и мониторинга

Рис. 3

В III квартале 55% событий с ИИ-маркерами относились к семейству OpenAI (ChatGPT, Codex), ещё 23% — к Meta AI*. Такой срез помогает отслеживать, какие инструменты чаще обращаются к защищаемым ресурсам и для каких из них стоит заранее определить политику доступа.

Какие семейства чаще встречались в заголовках запросов



Доля семейства во всех событиях с ИИ-маркерами, III квартал

Рис. 4

С ИИ-маркерами приходят и признаки эксплуатации

Внутри потока с ИИ-маркерами доля событий по правилам, связанным с эксплуатацией, **выросла с 1,1% во II квартале до 5,6% в III** (примерно в 5 раз). Чаще всего фиксировались SQL-инъекции, попытки обхода каталогов и командные инъекции — на них пришлось около 59%, 24% и 10% соответственно.

Структура событий за период также изменилась: во II квартале чаще встречались признаки раскрытия данных, а в III квартале наибольшая доля событий пришлась на правила обнаружения автоматизированных обращений. Также выросли доли срабатываний, связанных с доступом к служебным данным и возможной эксплуатацией уязвимостей. Это показывает, что запросы с ИИ-маркерами затрагивают разные механизмы защиты.

Как изменился состав событий с ИИ-маркерами

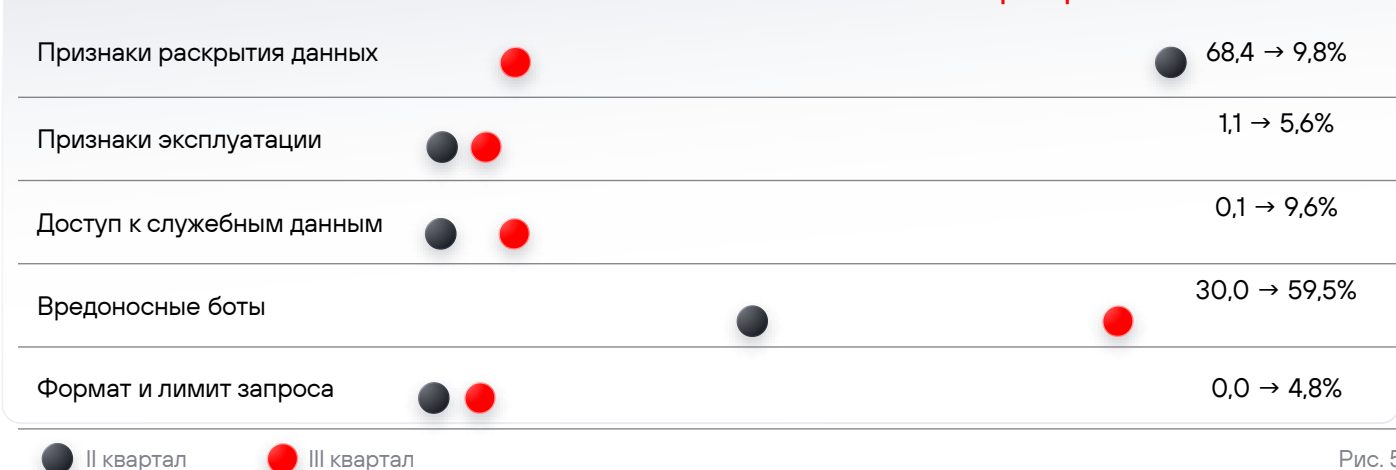


Рис. 5

Доля браузероподобных заголовков (например, Chrome, Safari) среди всех событий безопасности **выросла с 38,8% до 51,3%**. Браузерный заголовок одинаково характерен и для человека, и для автоматизированного сканера. Также увеличилась доля заголовков, характерных для ботов и средств автоматизации. При этом доля заголовков, характерных для приложений и SDK, напротив, сократилась почти вдвое.

Какие типы заголовков встречаются

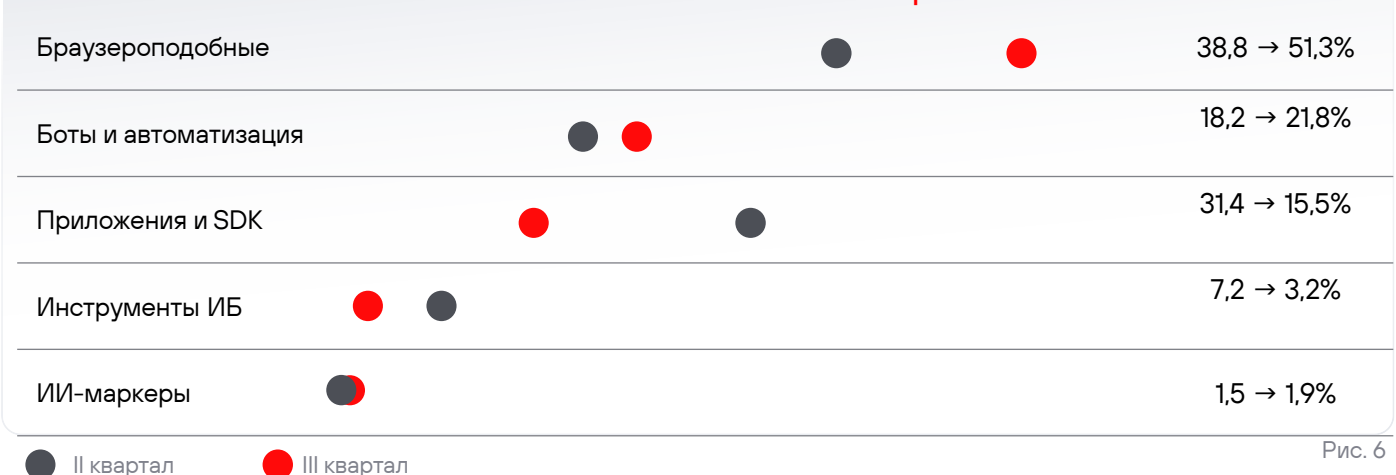


Рис. 6

React2Shell напоминает о себе спустя месяцы

Команда React раскрыла 3 декабря 2025 года критически опасную уязвимость, связанную с удаленным выполнением кода, в React Server Components — **CVE-2025-55182 с максимальной оценкой 10 по шкале CVSS**. Вскоре появились публичные способы ее эксплуатации и были зафиксированы попытки атак.

PT AF Cloud фиксировал попытки эксплуатации уязвимости с момента её публичного раскрытия. Существующие механизмы защищали клиентов от эксплуатации и по мере появления новых техник эксплуатации мы обновляли правила детектирования. Ниже приводим статистику по React/Next.js за II и III кварталы.

Число **событий, связанных с React/Next.js, выросло в 3,2 раза в августе и в 6,3 раза в сентябре**. Публичный PoC упростил автоматизацию проверок, поэтому сканеры могли продолжать обращаться к распространённому стеку в течение нескольких месяцев.

Динамика событий, связанных с React/Next.js



Рис. 7

У каждой уязвимости свой календарь

В III квартале число событий в React/Next.js, связанных с попытками добиться удаленного выполнения кода, отказа в обслуживании и раскрытия исходного кода, вдвое превысило показатель II квартала.

Активность по другим уязвимостям достигала пика в разные месяцы:

- Apache HTTP Server — в мае
- PHP CGI — в сентябре
- Spring4Shell — в апреле

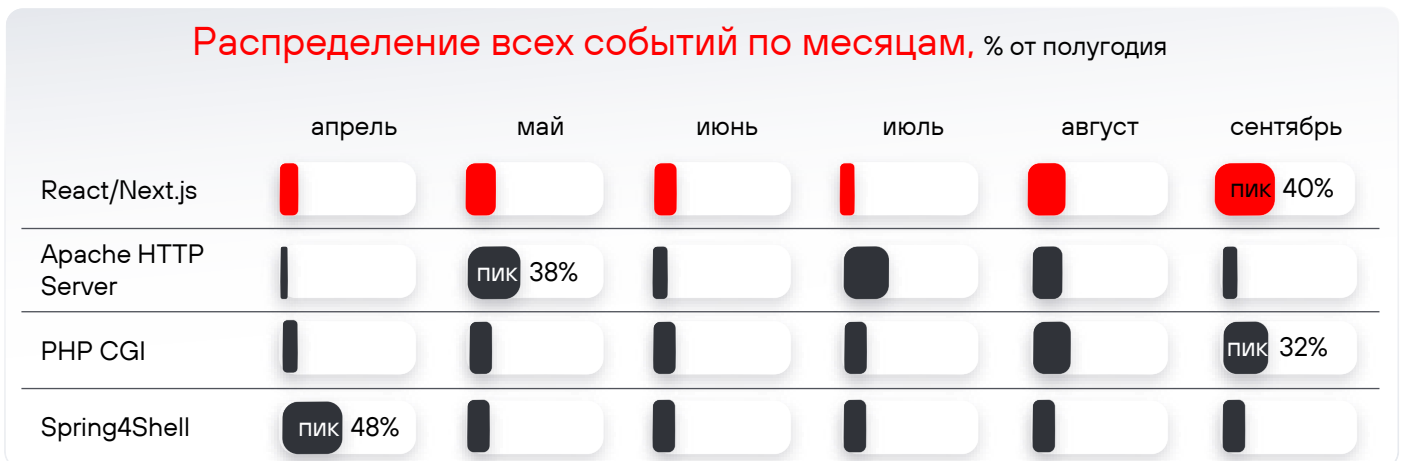


Рис. 8

Известные уязвимости продолжают привлекать внимание атакующих спустя месяцы и даже годы после раскрытия.

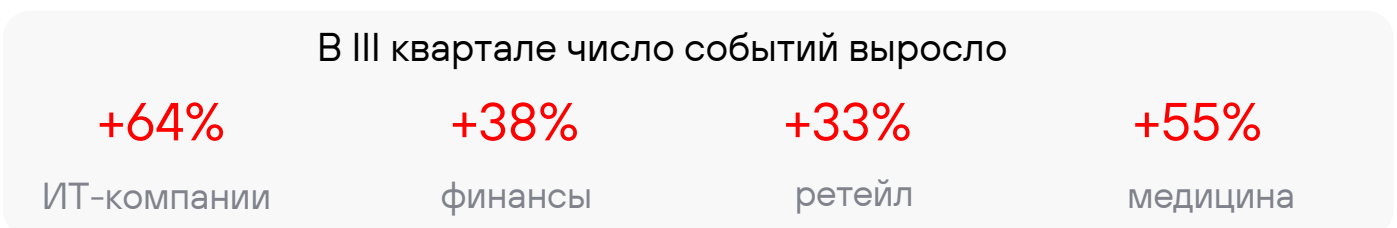
Для команды безопасности вывод прост: важно не только своевременно устанавливать обновления, но и контролировать попытки эксплуатации известных уязвимостей, сопоставляя их с используемыми технологиями и версиями ПО.

Отдельная волна вокруг Fortinet

В III квартале мы зафиксировали резкий рост числа событий, связанных с уязвимостями Fortinet. Число событий в **августе было в 47 раз выше июльского, а в сентябре — в 65 раз.**

Такая динамика может указывать на массовое автоматизированное сканирование: злоумышленники проверяют доступные ресурсы на наличие известных уязвимостей, зачастую без предварительного определения используемых технологий. Поэтому подобные запросы могут фиксироваться даже на ресурсах, которые не используют решения Fortinet.

Отрасли видят разные изменения



В СМИ показатель почти не изменился, в промышленности и транспорте снизился. Единого отраслевого сценария нет — динамика зависит от состава защищаемых ресурсов и того, какие правила срабатывают на них.

Изменение числа событий безопасности в наблюдаемых отраслях

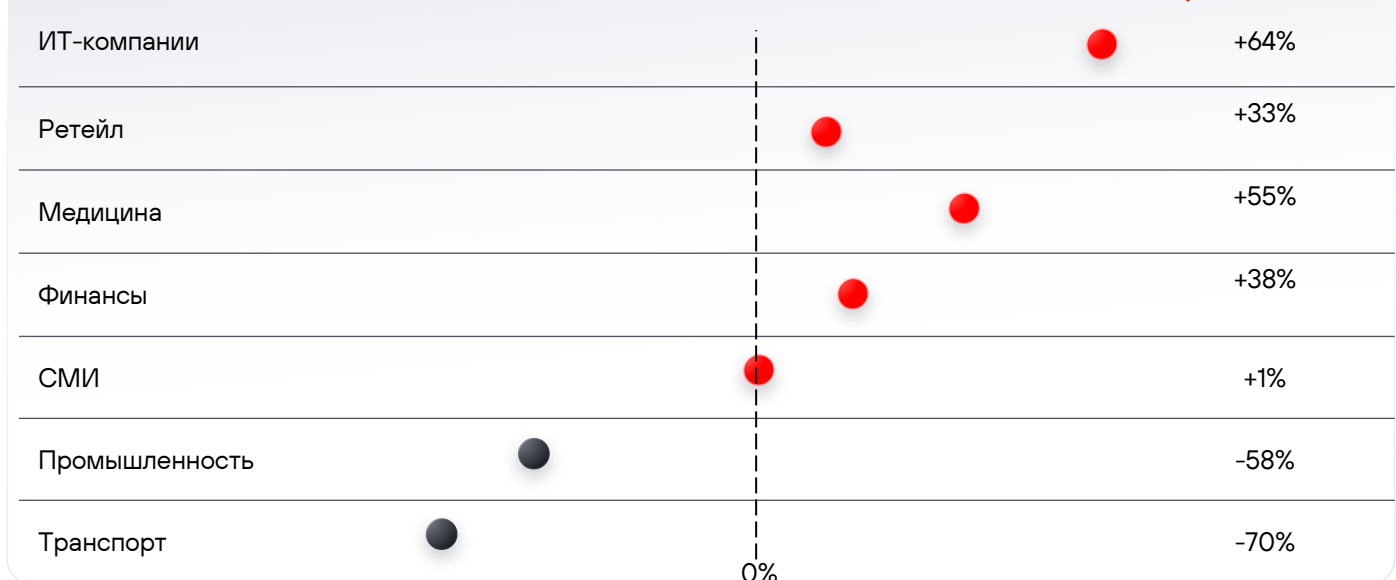


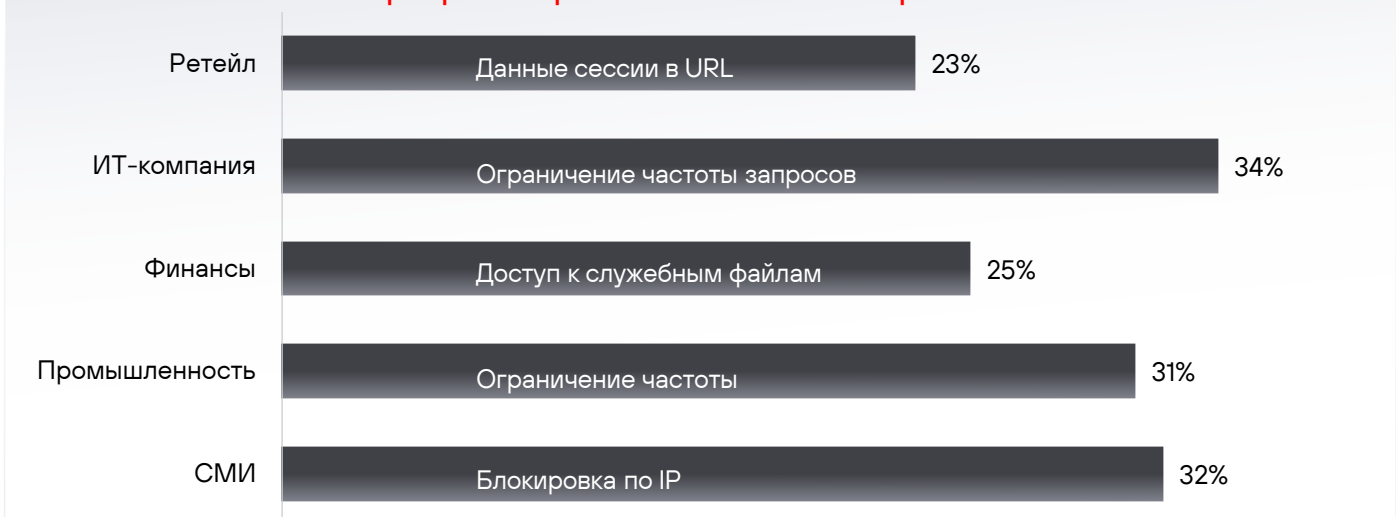
Рис. 9

Динамика числа событий неоднородна и сама по себе не раскрывает характер подозрительной активности. Поэтому мы отдельно проанализировали, какие правила защиты чаще всего срабатывали у клиентов из каждой отрасли в III квартале.

У каждой отрасли свой профиль срабатываний

В ретейле чаще других срабатывало правило о данных сессии в URL; в финансах — об обращении к служебным файлам; в ИТ и промышленности — об ограничении частоты запросов, в СМИ — о блокировке по IP-адресу. Поиск наиболее частого правила в своей отрасли помогает выбрать сценарий для проверки, а не строить рейтинг самых атакуемых объектов.

Профиль срабатываний по отраслям



Ведущее правило и его доля среди всех событий отрасли, III квартал

Рис. 10



Вторые по частоте сигналы добавляют детали: в ретейле — проверка CSRF-токена, в ИТ — автоматизированные User-Agent, в финансах — ограничение частоты, в промышленности — некорректный Content-Type, в СМИ — повторяющийся заголовок запроса. Эти данные можно использовать как отправную точку для проверки аналогичных сценариев в собственных приложениях.

Что проверить у себя

Регулярное обновление инфраструктуры помогает устранять уязвимости, но не защищает от всех видов автоматизированной активности. Даже к стабильно работающим приложениям непрерывно идут автоматизированные запросы, создающие избыточную нагрузку и риски для бизнеса.

Проверьте, какие запросы получает ваше приложение. Начните с анализа журналов веб-сервера или балансировщика. Обратите внимание на массовые обращения к несуществующим страницам, попытки доступа к служебным файлам, аномальную частоту запросов и повторяющиеся ошибки авторизации. Такие признаки помогут выявить сканирование и другие виды автоматизированной активности.

Разделяйте полезную и нежелательную автоматизацию. Поток ботов неоднороден: полезным роботам (поисковым системам, партнерским ИИ-сервисам) необходим доступ к контенту, тогда как нежелательную бот-активность надо пресекать. Определите, каким автоматизированным системам нужен доступ, а для остальных предусмотрите ограничения. Особое внимание уделите чувствительным операциям: авторизации, регистрации, поиску и обращениям к API.

Анализируйте поведение запросов. Для выявления автоматизации учитывайте частоту и последовательность обращений, повторяемость параметров и поведение клиентских сессий. Это поможет обнаруживать подозрительную активность, которая внешне выглядит как обычный браузерный трафик.

Оценить реальную видимость входящих запросов и проверить, атакуют ли вас можно на демонстрационном стенде PT AF Cloud demo.ptcloud.ru

О данных и источниках

Период исследования: 1 апреля — 30 сентября 2026 года.

Событие — запись о срабатывании механизма защиты, а не уникальная атака или весь HTTP-трафик.