Кибератаки на онлайн-ресурсы российских компаний в 1 полугодии 2026 года

Совместный отчет компаний WMX и Servicepipe

Москва, 2026

Оглавление

Введение

В первом полугодии 2026 года кибератаки на онлайн-ресурсы российских компаний стали не только более массовыми, но и значительно усложнились. Если раньше злоумышленники использовали отдельные техники – DDoS, эксплуатацию веб-уязвимостей или атаки на учетные записи, – то сегодня они все чаще объединяют их в многоэтапные кампании. Современная атака обычно начинается с автоматизированной разведки, затем переходит на инфраструктурное воздействие, после чего злоумышленники приступают к эксплуатации уязвимостей API, бизнес-логики и веб-приложений.

Настоящий отчет подготовлен на основе агрегированных данных компаний **WMX** и **Servicepipe**, собранных в первом полугодии 2026 года. В исследовании проанализированы основные этапы современных атак, изменение тактик злоумышленников, отраслевые особенности угроз и ключевые тенденции, которые будут определять развитие ландшафта киберугроз в ближайшей перспективе.

- Данные, представленные WMX, отражают ключевые веб-угрозы, которые были зафиксированы решением **ПроWAF** (межсетевой экран уровня веб-приложений).
- Данные, представленные Sevicepipe, фиксировались с помощью продуктов **DosGate, Cybert**, а также выявлялись в рамках **Лаборатории кибербезопасности Servicepipe.**

Ключевые тезисы

- **Переход к многосоставным атакам**

Главная тенденция первого полугодия 2026 года – это стирание границы между инфраструктурными DDoS-атаками и классическими веб-атаками. Все чаще фиксируются комбинированные кампании, где L3/L4-флуд используется как отвлекающий маневр, а основной ущерб наносится через эксплуатацию уязвимостей API, бизнес-логики и веб-приложений.

- **Рост автоматизации атак**

Количество веб-атак продолжает расти, а сами атаки становятся более автоматизированными и нацеленными на уязвимости в популярных фреймворках. Массовое применение ИИ, готовых эксплойтов и ransomware-as-a-service делает проведение сложных атак доступным даже для низкоквалифицированных злоумышленников.

- **Кибербразведка становится обязательным этапом атак**

Практически любому крупному инциденту предшествует этап разведки. К классическому «прощупыванию» периметра в 2026 году добавились активные попытки определить пороги срабатывания СЗИ.

- **Основная цель – бизнес-логика**

Веб-атаки смещаются с поиска технических уязвимостей на эксплуатацию бизнес-логики. То есть хакеры пытаются использовать функционал приложения против него самого. Основной канал эксплуатации бизнес-логики – это API.

Основные цифры

- **44%** крупных инцидентов представляли собой многоэтапные атаки, сочетающие DDoS и атаки на веб-приложения.

- **849,7 млн веб-атак** было отражено за 1 полугодие 2026 года (+27%);

- Количество автоматизированных сканирований периметра выросло более **чем в 2 раза**, что подтверждает роль кибербразведки в современных атаках.

- Доля DDoS-атак мощностью свыше **100 Гбит/с** увеличилась в пять раз, а максимальная мощность превысила **2 Тбит/с**.

- Число попыток удаленного выполнения кода (RCE) выросло **на 40%**, а злоумышленники все чаще атакуют API и бизнес-логику приложений.

Как злоумышленники атаковали веб?

Главная тенденция первого полугодия 2026 года – это **стирание границы** между инфраструктурными DDoS-атаками (L3/L4 по модели OSI) и классическими веб-атаками уровня L7 по модели OSI. Смешанные L4+L7 сценарии наблюдались примерно в **44% крупных инцидентов**.

В таких комбинированных кампаниях L3/L4-флуд часто используется как отвлекающий маневр (дымовая завеса), а основной ущерб наносится через эксплуатацию уязвимостей в API, бизнес-логике и веб-приложениях. Детектирование и локализация таких инцидентов сложнее, так как для защиты приходится одновременно закрывать несколько уровней.

Этап кибербразведки

Практически каждая сложная атака на онлайн-ресурсы в отчетном периоде начиналась с кибербразведки. Основной инструмент кибербразведки – это **автоматизированные сканирования**, число которых за год выросло **в 2 раза** (1H2025vs1H2026).

Сканирования – это попытки ботов и автоматизированных скриптов выявить уязвимости в веб-приложениях на периметрах компаний, что можно рассматривать как подготовительный этап к более сложным атакам, в том числе на социально значимые отрасли.

К классическому «прощупыванию» периметра в 2026 году добавились активные попытки определить **пороги срабатывания СЗИ**. Это техника slow-drip разведки – «тихое» сканирование. Используя низкоинтенсивные всплески (около 40 Мбит/с), атакующие прощупывают пороги срабатывания антиDDoS-систем (rate limits), чтобы затем нанести точечный удар.

Рост автоматизации связан с:

- развитием сервисов типа ransomware-as-a-service;
- распространением наборов эксплойтов, скриптов для сканирования;
- появлением ИИ помощников и агентов.

Это делает автоматизацию доступной даже для низкоквалифицированных злоумышленников.

С другой стороны, растет число веб-порталов, API, промышленных веб-интерфейсов и облачных сервисов, что делает ручные атаки малоэффективными. Чтобы найти «свою» уязвимость, атакующим выгоднее массово сканировать инфраструктуру, а затем отбирать наиболее перспективные точки входа.

Такой массив сканирующих запросов **усложняет детектирование**. На фоне миллионов автоматизированных, но не всегда успешных попыток эксплуатации сложнее выявлять действительно целевые цепочки атак, где к разведке добавляются сложный фишинг, 0-day-уязвимости и дальнейшее движение по сети.

Этап DDoS-атаки

Первая половина 2026 года характеризовалась переходом к **гиперобъёмным атакам.** Доля DDoS свыше 100 Гбит/с выросла в 5 раз: **с 3% до 15% год к году**.

- Абсолютный рекорд был зафиксирован в I квартале — мощность атаки превысила **2 Тбит/с.**
- Во II квартале зафиксирован инцидент мощностью **965 Гбит/с** при пакетной интенсивности свыше 100 млн пакетов в секунду (Mpps).
- В других крупных атаках пиковая нагрузка варьировалась **от 105 до 512 Гбит/с**.

Злоумышленники целенаправленно оптимизируют атаки для перегрузки CPU сетевого оборудования. В ряде точечных атак на веб-сегменты зафиксировано критическое соотношение: **генерация 33,3 Mpps при объёме всего 27,9 Gbps.**

Также наблюдается резкий рост **длительности инцидентов**. Если ранее атаки длились минуты, то сейчас фиксируются непрерывные сессии от 22 до 36 часов.

Типы DDoS и их динамика

UDP-флуд. Присутствовал в 100% крупнейших терабитных инцидентов как базовый инструмент исчерпания ёмкости каналов (включая использование отражающих NTP/DNS векторов).

TCP-аномалии (SYN-флуд, ACK-PSH). Зафиксированы в 78% случаев. Применялись для истощения таблиц состояний (state-table exhaustion) на классических межсетевых экранах.

Смешанные атаки (L4 + L7): Злоумышленники используют UDP/SYN-флуд как шумовую завесу для отвлечения внимания систем защиты, параллельно запуская узконаправленные запросы на уровень приложений (зафиксировано в 44% атак).

География и источники DDoS

Основной объём мусорного трафика генерируется распределёнными ботнетами с применением IP-спуфинга (подмены адресов).

Топ-10 стран-источников: Россия, Украина, США, Бразилия, Нидерланды, Франция, Аргентина, Великобритания, Индия и Чехия.

Особенности инфраструктуры. Фиксируется рост использования легитимных облачных провайдеров (AS-сетей) в качестве ретрансляторов для обхода GeoIP-блокировок.

Технические особенности DDoS-атак первой половины 2026

1. Все чаще злоумышленники стараются вывести из строя **теневую инфраструктуру**, направляя мусорный трафик в слепые зоны периметра. Например:

- неиспользуемые технические подсети (до 83,1 Gbps мусорного трафика);
- резервные каналы и VPN-концентраторы (RAVPN);
- среды разработки (dev-сегменты).

2. Атаки все чаще **синхронизируются с бизнес-часами** жертв или проводятся ранним утром перед релизами для максимального ущерба.

3. Одной из доминирующих тактик стали **ковровые атаки**, нацеленные не на конкретный IP-адрес, а на целые диапазоны и подсети (включая сотни и тысячи IP-адресов). За счёт «размазывания» мусорного трафика равномерно по всему пулу адресов, злоумышленники **обходят** классические rate limits, настроенные на защиту одиночных хостов. В первом полугодии этот метод использовался злоумышленниками особенно активно: мусорный трафик рассеивался как по основным публичным адресам, так и по теневой инфраструктуре (резервные каналы, dev-среды, B2B-шлюзы). Это подтверждает общую тенденцию рынка – атаковать не конкретный сервис, а выводить из строя инфраструктуру на уровне всего провайдера или дата-центра.

4. Новый вектор истощения - **импульсные (серийные) атаки**. В отчетном периоде фиксировался резкий всплеск коротких, но экстремально мощных импульсных атак – **на 20%.** Такой DDoS-удар длится всего 45–60 секунд, но повторяется каждые 5–10 минут. Поскольку классические системы защиты детектируют аномалии только на отрезке «от 1 минуты и более», импульсные волны успевают «пробивать» периметр. В то же время решения Servicepipe детектируют такие атаки за 1 секунду. Наибольшее давление от этого вектора испытывает:

- телеком (где доля таких атак достигла 80% от всех инцидентов);
- e-commerce (55%);
- финансовый сектор (42%).

Этап эксплуатации веб-уязвимостей

В 1 квартале 2026 года межсетевой экран уровня веб-приложений WMX ПроWAF отразил 412 млн атак, во 2 квартале 437 млн. Суммарно за полгода было отражено **849,7 млн. попыток атак** на онлайн-ресурсы клиентов. Динамика атак год к году:

	2025	2026	динамика
1 Q	334 010 214	412 481 181	+19%
2 Q	282 210 637	437 274 380	+35%
1H	616 220 851	849 713 611	+27%

Техники и тактики веб-атак

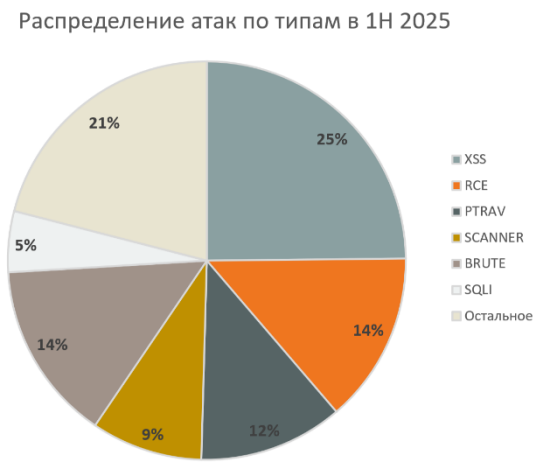
1. Крупный блок угроз в 1 половине 2026 года был связан с **инъекционными атаками** (например, XSS, SQLi, SSTI). Суммарно за год их количество выросло на четверть.

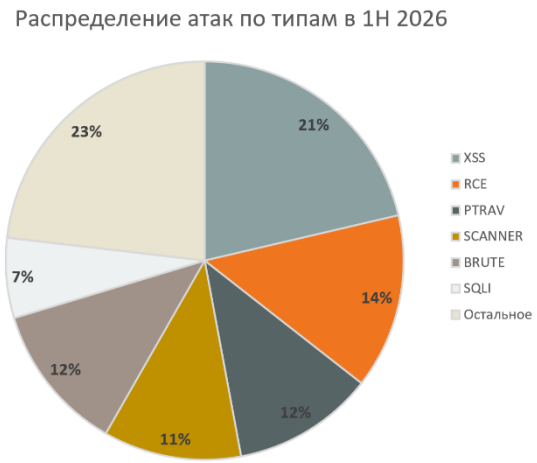
- **XSS** при этом остается самой распространенной веб-угрозой для бизнеса. По итогам 2025 года на XSS пришлась треть всех атак, в 1 полугодии 2026 года доля XSS – 20%.
- На втором месте – попытки **удаленного выполнения кода на серверной части приложений** (RCE), число которых выросло на 40% год к году. Это наиболее опасный тип веб-атаки, т.к. он позволяет не просто получить контроль над всем приложением, но и распространить атаку дальше на другие сегменты корпоративной сети.
- Высокая доля RCE (а также Path Traversal) свидетельствует о том, что атакующие продолжают инвестировать усилия в поиск именно таких уязвимостей, которые позволяют либо моментально захватить контроль над сервером, либо получить конфиденциальную информацию для дальнейшей компрометации.

2. Отдельно отмечается рост **атак на бизнес-логику приложений и API**. Это использование функционала приложения против него самого. Успешные атаки на бизнес-логику трудно обнаружить обычными средствами, что делает их воздействие особенно разрушительным. Эти техники все чаще используются не для компрометации инфраструктуры, а для манипуляции пользовательскими сценариями: платежами, авторизацией, бонусными программами и внутренними бизнес-процессами компаний.

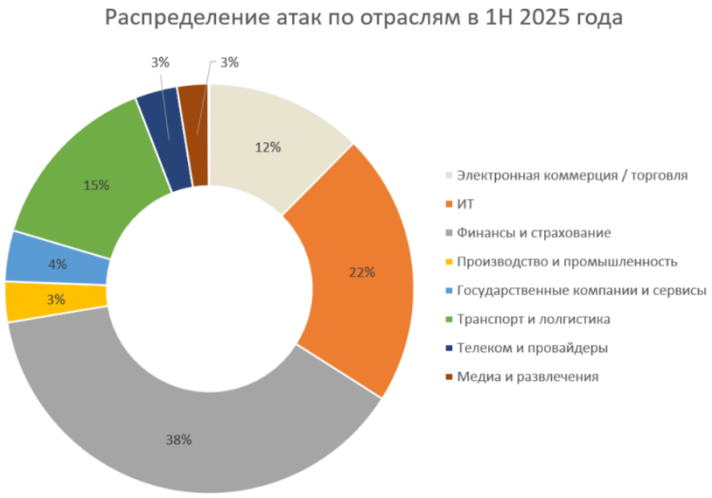
   Основные цели таких атак – критичные бизнес-процессы (авторизация, регистрация пользователей, платежные сценарии, программы лояльности). **Основной канал эксплуатации** логических уязвимостей – API (программный интерфейс, через который приложения и сервисы обмениваются данными).

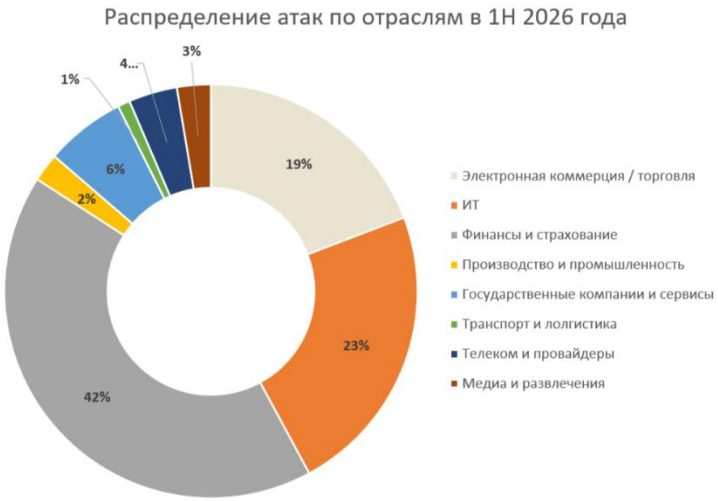
Через них атакующие автоматизируют подбор сценариев, обход ограничений, массовое выполнение операций и атаки на учетные записи.





Какие отрасли стали драйверами роста веб-атак





1. **Финансы и страхование**

- крупнейший абсолютный рост среди отраслей;
- финсектор остается главной целью атакующих;
- драйверы роста: Path Traversal, XSS и Брутфорс.
- фокус злоумышленников сместился с инфраструктуры на доступ, пользовательские сессии и API, где ущерб наступает быстрее и детектируется сложнее.

2. **Электронная коммерция**

- сильный рост атак на клиентские интерфейсы и платежные потоки;
- традиционные массовые атаки либо стабилизировались, либо стали менее эффективны. Снижается XSS, брутфорс, сканирования. Хотя XSS, несмотря на снижение, остается доминирующей атакой на отрасль;

- но резко растут точечные и более «дорогие» векторы: SQL, dirbust, XXE. Рост SQLi говорит, что атакующие стали чаще бить именно по backend-логике и к интеграциям (потенциал для supply-chain).

3. Госсектор

- почти удвоение, вероятно из-за усиления политически мотивированных кампаний;
- топ-атак: XSS, брутфорс, сканнер, RCE, Path traversal.

3. ИТ-компании и провайдеры облачных услуг

- традиционно страдают от SQL-инъекций и массового бот-сканирования;
- ИТ атакуют ради цепочек поставок (supply-chain), провайдеров – ради инфраструктурного контроля и клиентского доступа.

Бот-атаки на всех уровнях

Если раньше автоматизированные боты использовались преимущественно для массового перебора учетных данных или простого сканирования веб-ресурсов, то в 1 полугодии 2026 года они превратились в универсальный инструмент сопровождения практически **всех этапов атаки**.

На этапе разведки именно автоматизированные системы выполняют массовое сканирование веб-периметра, поиск новых API, определение версий ПО, тестирование механизмов защиты и порогов срабатывания средств безопасности. Рост количества подобных сканирований за год превысил двукратный уровень.

На **этапе эксплуатации** веб-уязвимостей боты автоматизируют поиск уязвимостей, эксплуатацию типовых ошибок конфигурации, подбор сценариев атак на API и массовые попытки эксплуатации известных уязвимостей.

Одновременно меняется качество автоматизации. Все чаще используются интеллектуальные боты, способные имитировать поведение реальных пользователей: корректно работать с cookies и TLS-отпечатками, соблюдать ограничения по частоте запросов, менять профиль активности и тем самым затруднять обнаружение средствами защиты.

В результате бот-трафик перестает быть самостоятельной угрозой и становится базовой инфраструктурой для проведения многоэтапных атак – от разведки до эксплуатации бизнес-логики приложений.

Новые типы ботовых атак в 1 полугодии 2026 года

Обход двухфакторной аутентификации

Выявлен новый способ атаки, позволяющий обходить механизмы двухфакторной аутентификации для входа в различные аккаунты по одноразовому коду (OTP) из СМС. При незначительной модификации логики автоматизированные боты способны не просто генерировать СМС-нагрузку, но и получать коды для авторизации через подбор (брутфорс). Цель новой атаки ботов – подобрать значения коротких OTP и войти в аккаунты. Таким образом злоумышленники могут получить доступ к чувствительным персональным данным пользователя, в том числе к платежной информации. При использовании коротких OTP-кодов и недостаточных защитных механизмах вероятность успеха атаки возрастает.

Двухэтапные атаки

Ещё один тренд первого полугодия 2026 года – **рост двухэтапных атак** (связки brute force и credential stuffing): на 35% в сегменте онлайн-торговли и на 23% в финансовом секторе с начала года.

Причина роста в резком удешевлении инструментария для атак. Теперь злоумышленники могут эффективнее комбинировать credential stuffing с точечным подбором паролей на основе открытых данных о пользователях. Хакеры используют ИИ-инструменты для вычисления логинов и паролей на слабо защищённом ресурсе и затем в автоматическом режиме проводят атаки credential stuffing с целью входа в личный кабинет.

По мере удешевления ИИ-инструментов спрос на массовые базы паролей для атак типа credential stuffing может начать снижаться. Более полные базы данных (с именами, телефонами, адресами, номерами паспортов), вероятно, сохранят ценность для телефонного мошенничества и целевого фишинга – там важна личная информация о жертве, а не пароль от аккаунта.

Намеренные ошибки ботов при прохождении CAPTCHA

При ботовых атаках в большинстве случаев атаки шли со стороны так называемых продвинутых ботов, мимикрирующих под легитимных посетителей сайтов. Перед тем как идти в API продвинутые боты делают запросы к динамике/статике. Также боты часто:

- прощупывают рейт-лимиты;
- ходят ровно ниже рейт-лимита (например, 15 запросов в минуту, все ботовые IP идут с рейтом 14 и т. д.);
- используют валидные заголовки (Headers);
- собирают корректные файлы cookie;
- формируют легитимные TLS/JA3 отпечатки (fingerprints).

Помимо этого, боты стали намеренно ошибаться при прохождении CAPTCHA – автоматизированного теста на сайтах, призванного отличить действия ботов от людей.

Выводы

1. **Главным трендом первого полугодия стал переход к многоэтапным атакам.**

   Все чаще злоумышленники комбинируют разведку, DDoS, эксплуатацию веб-уязвимостей, атаки на API и бизнес-логику. Это существенно усложняет обнаружение инцидентов, поскольку защита должна одновременно работать на сетевом, прикладном и бизнес-уровне.

2. **Разведка становится обязательной частью практически каждой сложной атаки.**

   Количество автоматизированных сканирований выросло более чем в 2 раза. При этом злоумышленники исследуют не только инфраструктуру компании, но и эффективность средств защиты, определяя наиболее удобные точки входа.

3. **Боты становятся основным инструментом атакующих.**

   Автоматизация сопровождает практически все этапы атаки – от поиска уязвимостей до эксплуатации API и бизнес-процессов. Использование ИИ делает подобные инструменты доступными даже для злоумышленников с невысокой квалификацией.

4. **DDoS все чаще используется как часть комплексной атаки.**

   Инфраструктурное воздействие применяется не только для нарушения доступности сервисов, но и для отвлечения внимания специалистов ИБ во время эксплуатации веб-приложений.

5. **Основная цель атак постепенно смещается с инфраструктуры на приложения и бизнес-процессы.**

   Рост числа RCE, атак на API и случаев эксплуатации бизнес-логики показывают, что злоумышленники стремятся не столько вывести сервис из строя, сколько использовать его штатную функциональность для получения финансовой выгоды или доступа к данным.

6. **Классической защиты веб-приложений уже недостаточно.**

   Эффективная защита требует объединения средств противодействия DDoS, WAF, API Security, антибот-решений и поведенческого анализа.