kaspersky

Обзор 2026

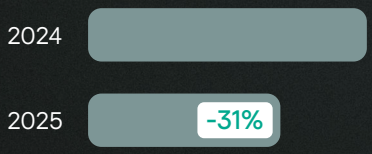
Киберпульс России

Специально
для ПМЭФ-2026

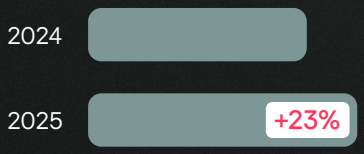
Ключевая статистика киберугроз для бизнеса в России

Количество кибератак на бизнес в России, 2025 vs 2024[1]

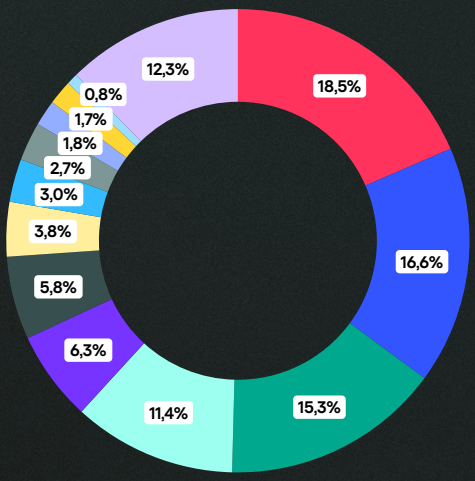
Веб-угрозы



Угрозы на устройстве



Распределение инцидентов высокой критичности по отраслевым секторам. Глобальная статистика[2]



Доля критичных инцидентов в ИТ отражает тренд на атаки на цепочки поставок. Инциденты в госсекторе — следствие геополитической напряженности. Потенциально высокая цена ИБ-инцидента для организаций в таких отраслях как финансы, промышленность и транспорт традиционно вызывает повышенный интерес злоумышленников к этим отраслям.

Данные по основным типам угроз для бизнеса в России, 2025 vs 2024

+49%

рост количества атак с помощью шпионского ПО[1]

+55%

рост количества атак с помощью ВПО для кражи паролей[1]

Каждый десятый россиянин генерирует рабочие пароли с помощью ИИ. Чтобы снизить риски и не зависеть от сторонних сервисов, компаниям стоит внедрить корпоративный менеджер паролей: он безопасно создает и хранит уникальные пароли и помогает их вовремя менять[3].

+23% +39% рост в Q1 2026

рост количества атак с помощью банкеров (ВПО для кражи денежных средств через онлайн-доступ к банковским счетам)[1]

+61%

рост количества атак с помощью бэкдоров[1]

-0,5% +20% рост в Q1 2026

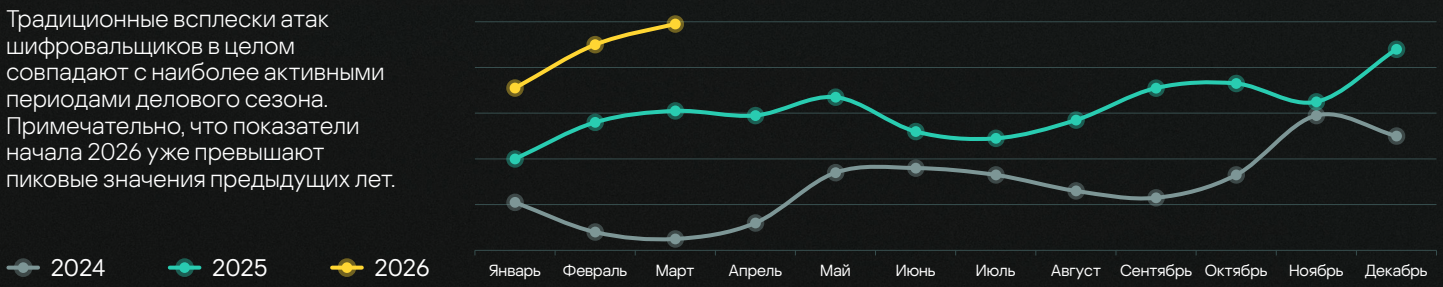
динамика количества атак с помощью программ-вымогателей (ransomware)[1]

-3% +39% рост в Q1 2026

динамика количества атак с помощью эксплойтов[1]

Сезонность атак с использованием программ-вымогателей на бизнес в России[4]

Традиционные всплески атак шифровальщиков в целом совпадают с наиболее активными периодами делового сезона. Примечательно, что показатели начала 2026 уже превышают пиковые значения предыдущих лет.



1 По данным Kaspersky Global Research and Analysis Team (GReAT)
2 По данным глобального отчета Kaspersky Security Services «Анатомия ландшафта киберугроз»
3 По данным исследования Kaspersky и hh.ru
4 По данным Kaspersky Cyber Threat Intelligence Team

Ландшафт киберугроз 2026: главные тренды

Кибершпионаж и коммерческое шпионское ПО

Инструменты для слежки, ранее доступные ограниченному кругу организаций, становятся массовой угрозой. Шпионское ПО «коммерциализируется» — его покупают, перепродают и применяют всё шире.

В 2025 году исследователи Kaspersky GReAT впервые зафиксировали в реальной атаке на российские организации применение коммерческого шпионского ПО Dante, созданного итальянской компанией Memento Labs (ранее Hacking Team). Чтобы избежать обнаружения, Dante использовало уникальный метод анализа среды, чтобы определить, может ли оно скрыто выполнять свои функции.

По следам сложнейшей атаки «Операция Триангуляция», раскрытой Kaspersky GReAT в 2023 году, был подробно описан шпионский инструмент Coruna. Он частично применялся в той атаке, а сегодня продолжает распространяться и угрожать iOS-устройствам.

+30

новых целенаправленных кампаний на организации в России с целью кибершпионажа

Атаки на цепочку поставок и доверительные отношения

Злоумышленники всё чаще атакуют не конечные цели напрямую, а разработчиков популярного ПО. Взломав один широко используемый продукт, можно заразить тысячи компаний одновременно. По данным Kaspersky, в 2025 году с такими атаками столкнулись 31% компаний в мире и 35% в России.

В мае 2026 года была обнаружена атака на DAEMON Tools: с начала апреля через официальный сайт распространялась версия программы со встроенным бэкдором. Заражено свыше 2 000 устройств в более чем 100 странах, 20% из них — в России, около 10% — корпоративные системы. В конце 2025 года аналогичная история произошла с Notepad++: с июля по октябрь 2025 года злоумышленники распространяли через него троян, постоянно меняя серверы управления.

По данным Kaspersky, к концу 2025 года в open-source-проектах по всему миру обнаружено почти 19 500 вредоносных пакетов — на 37% больше, чем годом ранее.

Отдельный тренд — атаки через доверительные отношения. Злоумышленники пытаются проникнуть в инфраструктуры крупных организаций через их подрядчиков, поставщиков, партнёров — небольшие компании с, как правило, более низким уровнем защищённости.

ИИ по обе стороны безопасности

Искусственный интеллект снижает порог входа в киберпреступность: теперь для сложных атак не нужна большая команда экспертов. ИИ помогает писать убедительные фишинговые письма, генерировать вредоносный код и автоматизировать разведку. Группировки вроде BlueNoroff уже применяют эти технологии для кражи криптовалюты.

В 2025 году зафиксирована волна атак Revenge Hotel: злоумышленники использовали ИИ для массовой рассылки персонализированных писем отелям — с поддельными жалобами, запросами документов и вложениями, содержащими вредоносное ПО. Вместе с этим компании активно внедряют ИИ-агентов для автоматизации бизнес-процессов. Прямое взаимодействие через ИИ-агентов расширяет поверхность атаки: злоумышленники ищут уязвимости в этих системах, чтобы проникать в цепочки партнёров. Поэтому внедрение ИИ-автоматизации требует системного и продуманного подхода.

только 25%

компаний включают безопасность ИИ в топ-5 приоритетов бизнеса

Исследование K2 и Kaspersky

Рекомендации ИБ на 2026 год

Дмитрий Галов
Руководитель
Kaspersky GReAT в России

Kaspersky GReAT: Глобальный центр исследования и анализа угроз

Kaspersky GReAT основан в 2008 году. В его задачи входит поиск и исследование наиболее сложных атак, кампаний кибершпионажа, новых методов заражения, эксплойтов, использующих уязвимости нулевого дня. Сегодня в команде центра более 30 экспертов, работающих по всему миру: в Европе, России, Южной Америке, Азии, на Ближнем Востоке. Они известны своими достижениями в расследовании наиболее сложных атак, включая кампании кибершпионажа и киберсаботажа.

Захватывающие истории мирового кибербеза — в новом подкасте от Kaspersky GReAT

Слушать

В ответ на ключевые киберугрозы «Лаборатория Касперского» советует организациям:

1 Внедрять модели нулевого доверия к цепочке поставок ПО

- Проверка цифровых подписей и хешей всех загружаемых обновлений
- Тщательные проверки и тестирование нового ПО перед развёртыванием
- Ведение реестра всех сторонних компонентов и open-source-зависимостей (SBOM)
- Мониторинг аномальной сетевой активности после любых обновлений

2 Настроить защиту от ИИ-усиленных атак

- Знакомство сотрудников с новыми реалиями кибербезопасности и соответствующее обучение
- Внедрение многофакторной верификации для финансовых операций и критичных запросов
- Использование ИИ-технологий для анализа поведения пользователей (UEBA) и предотвращения атак с подменой библиотек — боритесь ИИ против ИИ

3 Вести проактивный мониторинг уязвимостей

- Подписка на фиды актуальных уязвимостей и продвинутые данные Threat Intelligence
- Установка специализированного решения по управлению уязвимостями
- Внедрение виртуального патчинга для защиты до выхода официальных исправлений
- Регулярные пентесты с фокусом на свежие векторы атак

4 Обеспечить контроль периметра при внедрении ИИ-агентов

- Аудит всех точек интеграции ИИ-систем с внешними сервисами
- Ограничение прав доступа ИИ-агентов по принципу минимальных привилегий
- Логирование и мониторинг всех действий ИИ-систем
- Разработка плана реагирования на компрометацию ИИ-агента как отдельный сценарий

Кибербезопасность как стратегический актив

Современная ИБ — не только защита инфраструктуры, но и управление финансовыми рисками. Риск-ориентированный подход, разработанный «Технологиями доверия» для «Лаборатории Касперского», переводит киберриски и меры защиты в экономические метрики, помогая обосновывать бюджеты, расставлять инвестиционные приоритеты и говорить о кибербезопасности на языке бизнеса.

Исследование о ROI в ИБ

www.kaspersky.ru

#kaspersky
#активируйбудущее