kaspersky



Обзор 2026

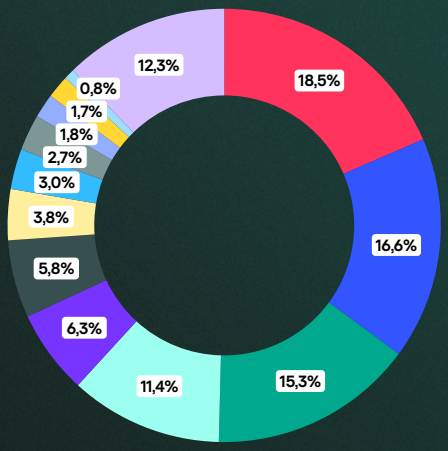
Киберпульс. Россия.

Ключевая статистика киберугроз для бизнеса в России

+54%

Общее количество киберинцидентов в российских организациях, I полугодие 2026 vs I полугодие 2025[1]

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



- Государственный сектор
- Промышленность
- ИТ
- Финансы
- Транспорт
- Образование
- Розничная торговля
- Здравоохранение
- Пищевая промышленность
- Телеком
- Разработка
- СМИ
- Прочее

Ландшафт киберугроз в России, I полугодие 2026 vs I полугодие 2025[3]

+24%
рост количества атак с помощью эксплойтов

+8%
рост количества атак с помощью бэкдоров

+56%
рост количества DDoS-атак (по данным Kaspersky DDoS Protection)

+3%
рост количества атак с помощью RDP-атак (атак на протокол удаленного рабочего стола)

-4%
снижение количества атак с помощью ВПО для кражи паролей

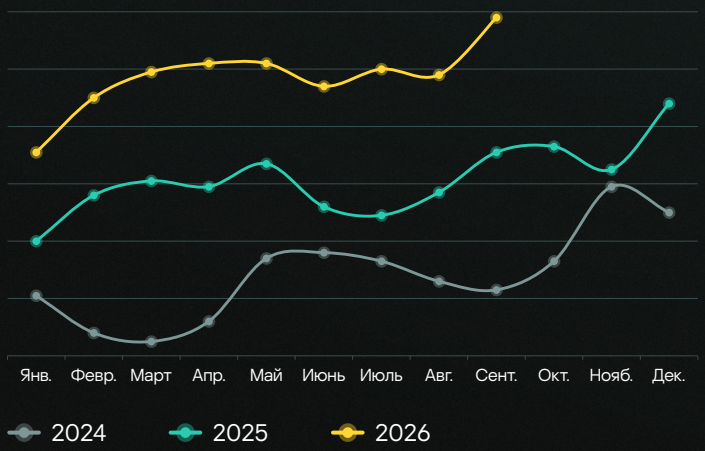
-0,5%
динамика количества атак с помощью банкеров (ВПО для кражи денежных средств через онлайн доступ к банковским счетам)



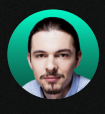
Дмитрий Галов
Руководитель Kaspersky GReAT в России

Рост в категориях «эксплойты» и «бэкдоры» отражает сдвиг к быстрым взломам уязвимых сервисов и «тихому» закреплению в сети для дальнейшего вымогательства и шпионажа. Это в том числе следствие роста количества уязвимостей нулевого дня и распространения технологий автоматизированного сканирования. Как только публикуется уязвимость или готовый эксплойт, злоумышленники тут же встраивают их в скрипты. Организации, которые не успели обновить ПО, рискуют столкнуться со взломом инфраструктуры. RDP-атаки были особенно распространены во время пандемии. Их возвращение в список значимых угроз связано с относительной простотой этого вектора первоначального доступа.

Динамика и сезонность атак с использованием программ-вымогателей на бизнес в России[4]



Шифровальщики — «классика» киберпреступности. На фоне развития технологий автоматизации и ИИ растут разнообразие, объемы, вариативность и кастомизация атак.



Фёдор Синицын
Эксперт группы исследований таргетированных атак

+9%
рост средней доли российских компаний, подвергшихся атакам с использованием программ-вымогателей (ransomware)[4]

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

Ландшафт киберугроз 2026: главные истории

Armored Likho: кибершпионаж в тренде

Подробнее

В мае 2026 года обнаружена кибершпионская кампания группы Armored Likho, нацеленной на крупные корпорации, государственный сектор, ИТ и образование, в том числе в России. Armored Likho проводит целевые атаки с новым модульным набором, который включает в себя загрузчики, бэкдоры и «стилеры», ориентированные на кражу данных мессенджеров, браузерных сессий и на скрытую прослушку через микрофон, перехват переписки/токенов мессенджеров и запись аудио. Всё это позволяет злоумышленникам следить за коммуникациями жертв в реальном времени.

Проникновение начинается с целевого фишинга с вредоносными ссылками или вложениями, после чего развёртывается полноценная цепочка атаки: закрепление в системе, связь с C2, развертывание «стилеров» и модулей прослушки. Финальная стадия — сбор чувствительных данных и постоянный удалённый доступ. Ключевая особенность этой кампании — прицельный фокус на закрепление в мессенджере и аудиошпионаж, что выделяет её среди типичных краж браузерных паролей и делает последствия более чувствительными для организаций и персональных коммуникаций.

+30

новых целенаправленных кампаний на организации в России с целью кибершпионажа

Hacking Cat: запутанный клубок атак хактивистов на организации в РФ

Подробнее

Hacking Cat — целевая кампания с «гибридным» набором инструментов: кастомный Gorilla RAT для удалённого управления, четыре варианта шифровальщика Monkey, деструктивный Nemo Wiper, коммерческий фреймворк для пентестов Cobalt Strike и шифровальщик ClearWater. Цепочка атаки: получение первоначального доступа через уязвимости в Exchange, закрепление и управление через Gorilla RAT/Cobalt Strike, скрытое продвижение по сети и финальный запуск шифрования (Monkey) или стирания (Nemo).

Особенность угрозы — сочетание вымогательских и уничтожающих операций, координация с другими хактивистскими группами. Злоумышленники используют разнообразные (зачастую самописные) инструменты и активно их дорабатывают. Например, многочисленные версии шифровальщика Monkey Ransomware появились в короткий промежуток времени. Это может, с одной стороны, говорить о том, что группировка экспериментирует с функциональностью, с другой — о применении вайбкодинга.

MovieReaper: заражение бизнес-организаций через торрент-раздачи

Подробнее

MovieReaper — модульный вредоносный фреймворк, распространяемый через скомпрометированный архив торрент-файлов. Вредоносные раздачи популярных фильмов, включая «Одиссею», приводили к загрузке троянца вместо ожидаемого контента. Кампания затронула сотни жертв по всему миру, включая российские организации ИТ, госсектора, консалтинг, розничную торговлю, транспорт и сельское хозяйство.

Цепочка атаки включает загрузчик, который проверяет среду выполнения и скачивает шеллкод, а затем использует блокчейн Solana для получения адреса C2-сервера. Далее вредоносное ПО обходит системные ограничения, закрепляется в системе и развёртывает модуль для удалённого управления файлами. Выполнение части кода в памяти затрудняет обнаружение. Ключевая особенность угрозы для бизнеса — возможность массово заражать пользователей сразу нескольких площадок и высокая устойчивость инфраструктуры злоумышленников. Риск также связан с заражением корпоративных устройств сотрудниками и последующим несанкционированным доступом к рабочим данным.



Захватывающие истории мирового кибербеза — в новом подкасте от Kaspersky GReAT

Слушать

Рекомендации ИБ на 2026 год



Анна Кулашова
Вице-президент «Лаборатории Касперского» по развитию бизнеса в России и странах СНГ

Искусственный интеллект становится новым рубежом в кибербезопасности, меняя как скорость и стоимость атак, так и подходы к защите. Злоумышленники уже используют ИИ для масштабирования атак, автоматизации разведки и создания более убедительных сценариев социальной инженерии. В то же время ИИ открывает новые возможности для проактивного выявления угроз, ускорения реагирования и повышения эффективности ИБ-команд. **Поэтому ключевой задачей становится адаптация систем кибербезопасности к новой реальности, в которой ИИ выступает одновременно мощным инструментом защиты и источником принципиально новых угроз.**

1 Безопасное внедрение и использование ИИ

- Встройте безопасность в ИИ с самого начала: правила, классификация данных и контроль доступа.
- Контролируйте данные и действия ИИ: защита от утечек, проверка результатов и ограничение полномочий.
- Управляйте рисками ИИ постоянно: мониторинг, оценка угроз и контроль соответствия требованиям.

Больше про ИИ в кибербезопасности

Безопасное внедрение облачных ИИ-агентов в процессы разработки

Безопасность ИИ-агентов через призму кибериммунитета

2 Быстрое и эффективное управление уязвимостями

- Срочно обновляйте внешние и ключевые системы; на критичные «дыры» — отдельный ускоренный процесс.
- Уменьшайте количество того, «что видно снаружи»: отключайте лишние функции и не публикуйте ненужные сервисы.
- Введите базовые запреты на рабочих местах: не запускать неизвестные программы, контролировать автозапуск.

3 Раннее выявление бэкдоров, туннелей и скрытого управления

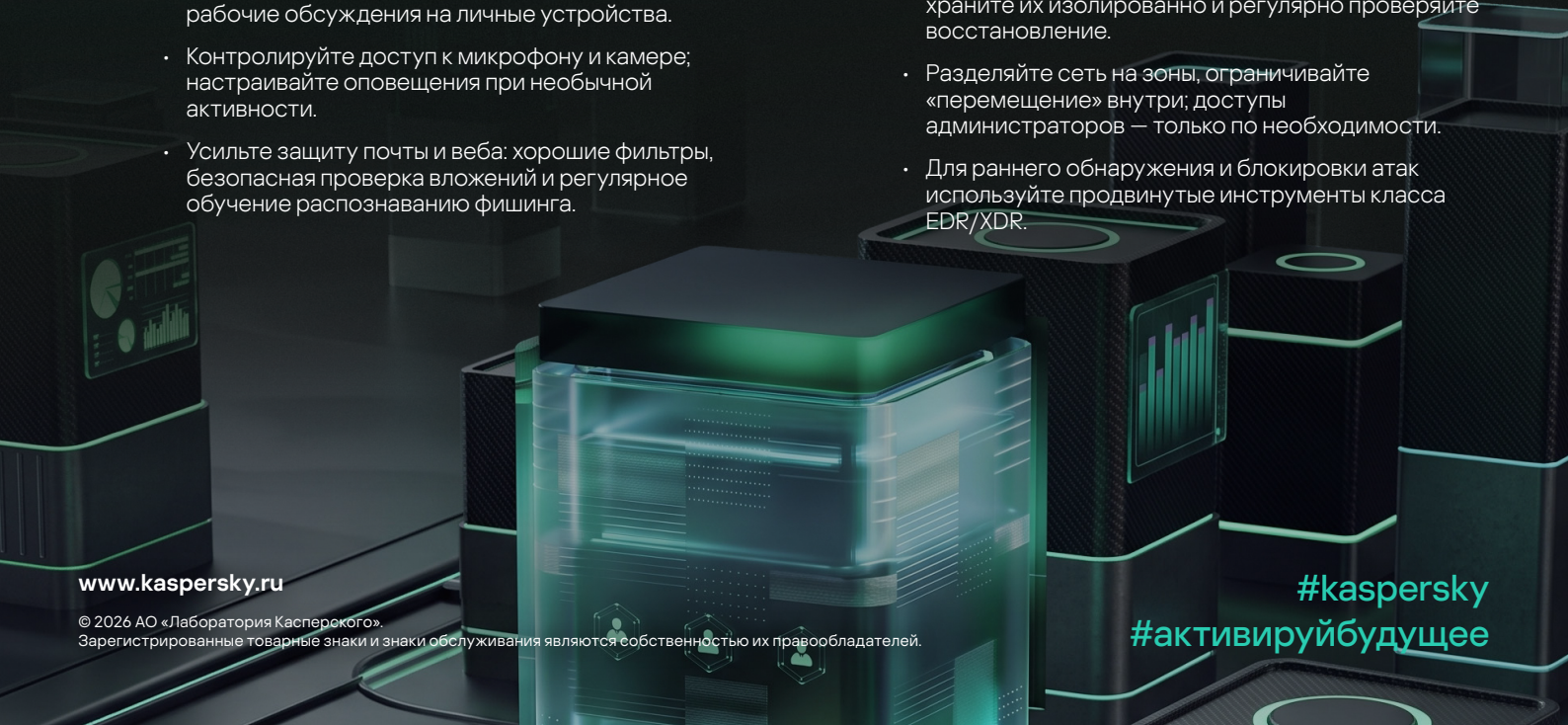
- Наблюдайте за необычными сетевыми соединениями и регулярными «тихими» выходами в интернет.
- Регулярно проверяйте важные серверы (например, почтовые) на следы посторонних изменений и новых служб.
- Защищайте инфраструктуру комплексно, собирая и коррелируя данные со всех ключевых элементов.

4 Защита рабочих станций и коммуникаций

- Берегите рабочие чаты и браузеры: используйте только официальные клиенты, не переносите рабочие обсуждения на личные устройства.
- Контролируйте доступ к микрофону и камере; настраивайте оповещения при необычной активности.
- Усильте защиту почты и веба: хорошие фильтры, безопасная проверка вложений и регулярное обучение распознаванию фишинга.

5 Противодействие шифровальщикам и «вайперам»

- Делайте резервные копии по понятным правилам, храните их изолированно и регулярно проверяйте восстановление.
- Разделяйте сеть на зоны, ограничивайте «перемещение» внутри; доступы администраторов — только по необходимости.
- Для раннего обнаружения и блокировки атак используйте продвинутые инструменты класса EDR/XDR.



www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее