

Как мы боремся с вредоносным ПО

Чтобы защитить пользователей от киберугроз, мы разрабатываем технологические решения и ведем просветительскую работу, помогая людям и бизнесу лучше понимать цифровые риски и способы защиты от них.

Почему это важно

По мере развития технологий растет и число киберугроз. В 2025 году решения Компании в среднем ежедневно обнаруживали 500 000 новых вредоносных файлов, что на 7% больше, чем в 2024 году. Эти цифры наглядно показывают масштаб угроз, с которыми сталкиваются пользователи и организации.

Эксперты отмечают, что кибератаки становятся все более сложными: злоумышленники используют уязвимости в программном обеспечении, украденные учетные данные, все чаще атакуют цепочки поставок и применяют инструменты на базе искусственного интеллекта. В таких условиях отсутствие надежной киберзащиты может привести к длительным простоям бизнеса и серьезным финансовым потерям, а для частных пользователей — к утрате данных и денежных средств.

Основные виды киберугроз

Наши решения защищают пользователей и организации от широкого спектра угроз. Среди них, например, разные виды вредоносных программ: [вирусы](#), [черви](#), [троянцы](#).

Вредоносные программы также можно классифицировать по их назначению — то есть по задачам, которые они должны выполнять для злоумышленников. Например:

- **шпионское ПО** может записывать происходящее вокруг жертвы на камеру и микрофон, отслеживать геолокацию, делать запись экрана, а также следить за активностью жертвы в мессенджерах и браузерах;
- **программы-стилеры** могут собирать и передавать злоумышленникам большие объемы конфиденциальной информации с зараженных устройств, например логины и пароли пользователя, данные платежных карт и криптовалютных кошельков;

- **шифровальщики** — это один из типов программ-вымогателей. Они представляют собой вредоносное ПО, которое шифрует данные на устройстве человека или компании и требует выкуп за дешифровку. Отдельная разновидность программ-шифровальщиков — **вайперы**. Их цель — безвозвратное уничтожение данных, и восстановление после такой атаки становится невозможным.

Киберугрозы могут классифицироваться и по способу распространения:

- **веб-угрозы** — вредоносное ПО, проникающее на устройства через интернет;
- **локальные угрозы** — распространяются через съемные носители или замаскированные установщики.

В 2025 году [веб-угрозы](#) были обнаружены на устройствах 34% пользователей в России (в мире — на 27%), а локальные угрозы — у 37% пользователей (в мире — у 33%). Основной мишенью злоумышленников остается Windows: с попытками атак столкнулись 48% пользователей операционной системы по всему миру. Для macOS этот показатель составил 29%.

В глобальном масштабе в 2025 году по сравнению с 2024 годом количество обнаружений программ для кражи паролей увеличилось на 59%, шпионского ПО — на 51%, а бэкдоров — на 6%.

Пользователи и компании также могут стать жертвой [фишинга](#), скама, телефонного мошенничества и [DDoS-атак](#).



Александр Лискин,

Руководитель управления исследования киберугроз в «Лаборатории Касперского»

«Уязвимости по-прежнему остаются самым популярным способом проникновения злоумышленников в корпоративные сети, за ними следует использование украденных учетных данных — отсюда рост числа и программ для кражи паролей, и программ-шпионов, который мы наблюдаем в этом году. Также распространены атаки на цепочку поставок, в том числе атаки на ПО с открытым исходным кодом. В этом году количество таких атак значительно возросло, и мы даже увидели первый широко распространенный NPM-червь Shai-Hulud».

Реагируем на рост количества мобильных угроз

Данные на смартфонах становятся одной из ключевых целей злоумышленников. В [общей сложности](#) в 2025 году Компания предотвратила более 14 млн атак с использованием мобильного вредоносного и нежелательного ПО в мире.

Самой массовой мобильной угрозой остается рекламное ПО — в 2025 году на него пришлось 62% всех выявленных случаев. Вместе с тем быстро растет число опасных троянцев. В России, например, в 2025 году одной из наиболее распространенных угроз для Android стал банковский троянец [Mamont](#), число атак которого выросло в десятки раз.

В отчетном периоде были выявлены и новые сложные мобильные угрозы — [SparkCat](#), [SparkKitty](#), [LunaSpy](#), которые маскировались под легитимные приложения и похищали данные пользователей, включая пароли и криптовалютные ключи. Опасность также представляют схемы с использованием [NFC](#)-троянцев: в третьем квартале 2025 года число атак с использованием таких зловредов в России выросло в 1,5 раза по сравнению со вторым. Телефонное мошенничество также остается массовым — в 2025 году с ним столкнулись 66% [пользователей в России](#).

Появились и модификации уже известных мобильных семейств, например обновленные версии банковского троянца [Necro](#) и известного троянца [Triada](#), который научился красть криптовалюту, перехватывать аккаунты в популярных мессенджерах и даже вмешиваться в телефонные звонки. Эти факты показывают, насколько быстро эволюционируют мобильные угрозы.



Дмитрий Галов,

Руководитель Kaspersky GReAT в России и странах СНГ

«Злоумышленники активно распространяли зловредные программы, в том числе в мессенджерах — под видом фотографий, трекеров для отслеживания доставки, приложений поддержки телеком-операторов, сервисов для получения медицинской помощи и не только».

Для защиты от телефонных мошенников Компания разрабатывает решение [Kaspersky Who Calls](#), которое уведомляет, если пользователю звонит возможный мошенник.

Чтобы уберечь смартфоны от киберугроз, мы рекомендуем их владельцам скачивать приложения только из официальных источников и использовать наши надежные защитные решения — [Kaspersky для Android](#) и [Kaspersky для iOS](#).

Защищаем от программ-вымогателей

Риски для бизнеса и частных лиц

Программы-вымогатели или шифровальщики (ransomware ПО) — один из самых опасных видов киберугроз для организаций. Их называют шифровальщиками, поскольку вредоносное ПО получает доступ к устройству, шифрует данные, а затем у пострадавших злоумышленники требуют выкуп.

Такие атаки могут парализовать работу компаний любого размера — от крупных корпораций до малого бизнеса, — и наносят ущерб во всех регионах. В 2024 году в России мы зафиксировали и предотвратили более 500 тысяч попыток атак с использованием шифровальщиков.

В глобальном масштабе доля пользователей, столкнувшихся с вымогательским ПО, сравнительно невелика (в 2024 году — [около 0,44%](#), что лишь на 0,02 п. п. выше, чем годом ранее). Это может объясняться тем, что злоумышленники не распространяют программы-вымогатели массово, атакуют точно по самым «ценным» жертвам — чаще всего по бизнесу, где потенциальный выкуп очень высок.

Цена реализованной атаки для бизнеса при этом выходит далеко за рамки выкупа — простой, сбой в цепочках поставок, ущерб репутации и последующие затраты на восстановление — все это может в разы превышать прямые выплаты злоумышленникам.

Совместно с VDC Research мы подсчитали потенциальные потери мировой промышленности от простоев из-за атак программ-вымогателей в первые три квартала 2025 года. По нашим оценкам, они могли превысить [\\$18 млрд](#) — причем это только потенциальный ущерб, вызванный простоем производственных линий.

В октябре 2025 года «Лаборатория Касперского» [зафиксировала](#) крупнейший за два года всплеск числа атак программ-вымогателей на российские организации, включая финансовые.

>\$18 млрд

возможная сумма глобального ущерба от атак вымогателей только за 9 месяцев 2025 года

>500 000 атак

на Россию с использованием программ-вымогателей зафиксировано за 2024 год

Новые тактики вымогателей

В 2024–2025 годах мы отметили несколько тревожных [тенденций](#), связанных с шифровальщиками:

- **активное использование ИИ** при создании вредоносного ПО;
- **преобладание модели RaaS** («ransomware как услуга»), когда отдельные группы разрабатывают программу-шифровальщик и сдают ее «в аренду» другим хакерам за долю от выкупа;
- **смещение атак к нестандартным точкам взлома**: вместо фишинговых писем или поиска уязвимости в веб-сервере злоумышленники теперь ищут нетривиальные пути: веб-камеры, IoT-устройства и другое плохо защищенное оборудование;
- **рост среднего размера выкупа** при одновременном снижении совокупных доходов злоумышленников. Так, в 2024 году средний размер выкупа вырос примерно в 1,5 раза по сравнению с годом ранее и достиг \$4 млн¹.



Наши решения

«Лаборатория Касперского» успешно помогает своим клиентам защищаться от постоянно усложняющегося ландшафта киберугроз.

Для организаций были созданы разные решения и [рекомендации](#) по кибербезопасности, позволяющие снизить киберриски таких атак и минимизировать ущерб.

Мы также разработали продукты, которые демонстрируют высокую эффективность против вредоносного ПО. Независимые тесты подтверждают, что решения Kaspersky Security для бизнеса, Kaspersky Small Office Security и продукты линейки решений Kaspersky для пользователей — [Kaspersky Standard](#), [Kaspersky Plus](#) и [Kaspersky Premium](#) — [эффективно](#) защищают пользователей.

В отчетном периоде решение [Kaspersky Standard](#) получило награду «Продукт с наивысшим рейтингом» (Top-Rated Product) от независимой лаборатории AV-Comparatives за 2024 год, набрав суммарно 100 баллов из 105 возможных. Компания удостоивалась этого звания уже шесть раз, а в 2023 году ее решение было [признано](#) «Продуктом года» в седьмой раз.

Решение [Kaspersky Premium](#) для Windows в 2025 году вновь получило сертификат качества (Approved) по итогам ежегодного антифишингового теста AV-Comparatives. Оно обнаружило 93% всех фишинговых ссылок и успешно прошло проверку на ложноположительные срабатывания.

Решение [Kaspersky Security](#) для бизнеса продемонстрировало 100%-ную защиту в тестах AV-Comparatives на защиту от несанкционированного доступа к учетным данным, успешно пройдя все 15 тестов. Решение Kaspersky EDR Expert было высоко оценено за достижение 100%-ного совокупного показателя активного реагирования (cumulative Active Response rate) в тестировании EDR-решений на качество обнаружения и предотвращения сложных угроз (Endpoint Prevention and Response Test) и было сертифицировано и награждено статусом «Стратегического лидера» в третий раз подряд.

В 2025 году Компания была удостоена [премии](#) «Лидеры кибербезопасности» сразу в трех номинациях. Жюри отметило развитие решения Kaspersky Container Security (KCS) для защиты контейнерных сред на всех этапах их жизненного цикла (к концу года реализовано более 30 проектов внедрения KCS), SIEM-платформу Kaspersky Unified Monitoring and Analysis Platform (KUMA) с интегрированным ИИ-ассистентом Kaspersky Investigation and Response Assistant (KIRA).

Также удостоены награды достижения Компании в области аналитики киберугроз — комплекс сервисов Kaspersky Threat Intelligence и высоко оценена ее работа по предоставлению организациям актуальных данных о техниках и тактиках злоумышленников для выстраивания проактивной защиты.

Помимо этого, «Лаборатория Касперского» продолжает активно участвовать в международной инициативе [No More Ransom](#), одним из основателей которой она является. Этот проект создан в 2016 году с целью помочь жертвам троянцев-вымогателей снова

получить доступ к своим зашифрованным данным, не выплачивая деньги атакующим. Участники альянса, включая Европол, нидерландскую полицию и вендоров из кибербезопасности, обмениваются опытом, знаниями и decryption tools — инструментами дешифровки, которые помогают восстанавливать данные, зашифрованные вымогателями.

Как мы закрыли лазейку для злоумышленников

Наши эксперты по расследованию инцидентов регулярно находят и устраняют слабые места, которыми пользуются вымогатели.

Мы участвуем в расследовании инцидентов, помогая закрывать уязвимости до того, как ими смогут воспользоваться злоумышленники.

В 2025 году при анализе атаки вымогателя MedusaLocker на одну из компаний в Бразилии специалисты «Лаборатории Касперского» выявили уязвимость в легальной утилите ThrottleStop, через которую вирус получил привилегированный доступ к системе.

Результат

Мы сразу сообщили об этой проблеме разработчику утилиты и оперативно добавили детектирование нового эксплойта в наши продукты, тем самым закрыв еще одну лазейку для вымогателей.

¹ По данным отчетности разработчика Sophos.

Предоставляем новейшие данные о киберугрозах

Для эффективного противодействия киберугрозам мы предоставляем организациям доступ к комплексу сервисов [Kaspersky Threat Intelligence](#), который содержит актуальные данные о тактиках, техниках и процедурах злоумышленников. Единая точка доступа к достоверным аналитическим данным об угрозах — Kaspersky Threat Intelligence Portal. Пользователям также доступна бесплатная версия портала — [Kaspersky Open TIP](#). Запросить доступ к этому сервису можно [здесь](#).

>200

закрытых отчетов о киберугрозах мы публикуем ежегодно

>900

групп и операций отслеживаем постоянно

Мы регулярно делимся инсайдами о кибератаках на профильных мероприятиях и в СМИ. К примеру, специалисты Глобального центра исследования и анализа угроз (Kaspersky GReAT) детально изучили активность группы [FunkSec](#), которая занимается двойным вымогательством (шифрует данные и одновременно ворует их), и опубликовали отчет о ее методах. Примечательно, что в создании своего вируса FunkSec активно применяла инструменты на базе ИИ.

Повышаем цифровую грамотность

«Лаборатория Касперского» проводит специальные исследования, опросы и обучающие кампании, чтобы повысить осведомленность о киберугрозах, с которыми люди сталкиваются в реальной жизни, часто даже не подозревая об этом.

В 2024–2025 годах в партнерстве с другими организациями мы выпустили несколько интересных исследований для широкой публики.

- [Совместно](#) с розничной сетью «М.Видео-Эльдорадо» мы выпустили документальный сериал [«Эволюция обмана»](#) на тему киберугроз и защиты от них. Сериал состоит из шести эпизодов по 10 минут. В нем эксперты и реальные герои рассказывают о схемах злоумышленников, психологических приемах социальной инженерии и способах защиты, помогая зрителям лучше понимать современные цифровые риски.

- В поддержку сериала Компания и «М.Видео-Эльдорадо» провели опрос и выяснили, что более половины россиян сталкивались с дипфейками — поддельными видео или аудио, созданными нейросетью. Мы рассказали, на что обращать внимание, чтобы не стать жертвой такого обмана.
- Вместе с «Почта Mail.ru» провели серию опросов о киберугрозах в электронной почте. Оказалось, [почти 50% россиян](#) получают подозрительные письма (которые относят к фишингу, скаму или спаму) каждый день, и при этом [половина опрошенных](#) уверена, что умеет отличить мошенническое сообщение (фишинговое и скам) от настоящего. При этом мы напомнили, почему

важно не только полагаться на собственные силы, но и использовать специализированные защитные решения. Другое исследование показало, что [более трети людей](#) готовы отказаться от привычных паролей в пользу беспарольных методов аутентификации — с использованием одноразовых и QR-кодов, отпечатка пальца или скана лица и других способов для входа в аккаунты. Мы рассказали о реально надежных способах защитить аккаунты.

- Совместно с отечественным магазином приложений RuStore [мы развенчали](#) популярные мифы о кибербезопасности смартфонов, помогая пользователям скорректировать опасные заблуждения и использовать устройства более безопасно.

Повышаем осведомленность бизнеса о киберугрозах

«Вы четко видите все риски?»

В 2025 году Точка Банк и «Лаборатория Касперского» совместно реализовали спецпроект [«Вы четко видите все риски?»](#) — интерактивный гид, ориентированный на предпринимателей из микро-, малого и среднего бизнеса.

Результаты

- **>2,5 млн** контактов узнали о проекте и задумались о проблеме
- **40 000** посещений составил трафик на сайт гида
- **>4 000** пользователей изучили реальные бизнес-риски

Наши планы на 2026–2027 годы

- Изучение фишинговых и спамерских схем и предоставление актуальной аналитики в новых отчетах
- Проведение и публикация исследований и опросов для информирования пользователей о разных киберугрозах, с которыми они могут столкнуться
- Выпуск ежегодного глобального отчета об атаках программ-вымогателей