

Как мы боремся с киберпреступностью

GRI 3-3

Масштабируя безопасность, мы развиваем глобальное сотрудничество с правоохранительными органами и профессиональным сообществом, усиливая экспертизу и помогая совершенствовать законодательство для борьбы с киберпреступниками.

Развиваем международное сотрудничество для противодействия киберпреступности

Современная киберпреступность не знает границ. Ни одна страна или организация не может справиться с этой угрозой в одиночку, борьба с ней требует объединения усилий. Вот почему мы активно сотрудничаем с международными организациями, государственными структурами и правоохранительными органами, помогая защищать людей и компании от киберугроз.

«Лаборатория Касперского» подходит к этому сотрудничеству прозрачно и ответственно. У нас есть четкий порядок работы с запросами от правоохранительных и государственных органов, который регулируется внутренней политикой. Каждый запрос проходит юридическую проверку по установленным критериям — при необходимости мы можем его отклонить или оспорить. При этом мы никогда не предоставляем доступ к нашей инфраструктуре или системам хранения данных пользователей.

Ключевые документы

- Внутренняя политика «Лаборатории Касперского», определяющая работу с запросами правоохранительных органов (утверждена в сентябре 2021 года топ-менеджерами Компании)
- [Соглашение с Интерполом](#) о совместной борьбе с киберпреступлениями в рамках проекта Gateway
- [Соглашение с Африполом](#) о сотрудничестве в сфере предотвращения киберпреступности и борьбы с ней
- Меморандумы о сотрудничестве с различными агентствами по кибербезопасности и правоохранительными органами

Проводим совместные операции с Интерполом и Африполом

«Лаборатория Касперского» с 2014 года сотрудничает с Интерполом в борьбе с киберпреступностью. В 2019 году мы также подписали соглашение в рамках проекта Gateway.

Наша поддержка правоохранительных организаций включает:

- обмен экспертной информацией о новейших видах вредоносных программ и методах кибератак;
- участие в совместных операциях по всему миру для выявления и пресечения киберпреступлений;
- обучение и консультирование сотрудников Интерпола и других правоохранительных органов в области кибербезопасности.

В 2024 году мы также формализовали сотрудничество с Африполом, подписав пятилетнее соглашение по противодействию киберпреступности в Африке.

Результаты совместных операций

>2 600

злоумышленников арестовано
в 2024–2025 годах

В отчетном периоде «Лаборатория Касперского» анонсировала результаты семи совместных операций с Интерполом и Африполом, в ходе которых было арестовано в общей сложности свыше 2 600 злоумышленников.

Операция [Synergia](#)

Сентябрь — ноябрь 2023 года

- Более 50 стран — членов Интерпола помо- гали выявлять и блокировать инфраструктуру для фишинга, распространения вредоносного ПО и атак программ-вымогателей.
- 31 человек задержан.
- 26 арестов в Европе, где находилась большая часть серверов.
- 153 сервера изъяла полиция Гонконга, 86 серверов — полиция Сингапура.
- Южный Судан и Зимбабве изъяли наибольшее число серверов на Африканском континенте и арестовали четверых человек.

Операция [Synergia II](#)

Апрель — август 2024 года

- Борьба с целевым фишингом, шифровальщиками и стилерами¹ по всему миру. В основном были затронуты страны Европы, Африки и Азиатско-Тихоокеанского региона.
- 100 подозреваемых выявлено, из них 41 арестован.
 - Около 30 тысяч подозрительных IP-адресов и серверов обнаружено (более 75% заблокировано).
 - Изъято 59 серверов и 43 электронных устройства.

Операция [Red Card](#)

Март 2025 года

- Проводилась в рамках проекта Интерпола по борьбе с киберпреступностью в Африке (AFJOC³) во взаимодействии с правоохрани-тельными органами семи стран (Бенин, Кот-д'Ивуар, Нигерия, Руанда, ЮАР, Того, Замбия). Число пострадавших от злоумышленников превысило 5 000.
- 306 арестов в регионе.
 - Около 2 000 устройств изъято.

Операция [Serengeti 2.0](#)

Июнь — август 2025 года

- Объединила правоохранные органы из 18 африканских стран и Великобритании для борьбы с программами-шифровальщи-ками, BEC-атаками и онлайн-мошенничеством. Жертвами злоумышленников стали около 88 000 человек.
- Более 1 200 подозреваемых задержано.
 - 11 432 объекта вредоносной инфраструктуры обезврежено.
 - \$97,4 млн — сумма возмещенного ущерба.

В ходе этой операции эксперты нашего Центра исследования угроз помогли раскрыть мошен-ническую схему с инвестициями в криптова-люту, из-за которой 65 000 человек потеряли в целом \$300 млн. В результате власти Замбии арестовали 15 человек.

Операция против [Grandoreiro](#)

Март 2024 года

Мы помогли Интерполу арестовать пятерых администраторов, управлявших банковским троянцем Grandoreiro, жертвами которых стали более 900 финансовых учреждений в более чем 40 странах Северной и Латинской Америки, а также Европы. Ущерб от действий злоумышлен-ников превысил €3,5 млн.

Операция [Serengeti](#)

Сентябрь — октябрь 2024 года

- Борьба с программами-шифровальщиками, BEC-атаками² через корпоративную электронную почту и другими преступлениями. Их жертвами стали более 35 000 человек, суммарный ущерб от их действий составил \$193 млн.
- Более 1 000 подозреваемых задержано
 - 134 089 объектов вредоносной инфраструктуры обезврежено

Операция [Secure](#)

Январь — апрель 2025 года

- Выявление и блокировка вредоносной актив-ности с использованием программ-стилеров в Азиатско-Тихоокеанском регионе.
- 26 стран и компании — партнеры Интерпола присоединились к операции.
 - Более 30 подозреваемых задержано (в том числе 18 — во Вьетнаме).
 - Более 20 тысяч нелегитимных IP-адресов и доменов заблокировано.
 - Свыше 40 серверов изъято.
 - Более 216 000 жертв уведомлены о необходи-мости немедленно принять защитные меры.

¹ Стилер — вредоносная программа, которая незаметно собирает большое количество конфиденциальной информации с зараженных устройств, например логины и пароли, данные платежных карт.

² BEC (Business Email Compromise) — это атака, при которой зло-умышленники начинают переписку с сотрудником компании с целью завоевать его доверие и убедить выполнить действия, идущие во вред интересам компании или ее клиентам.

³ African Joint Operations against Cybercrime.

Расширяем экосистему партнеров

Совместно с Интерполом «Лаборатория Касперского» обеспечивала кибербезопасность значимых событий.

- Летние Олимпийские игры 2024 года в Париже — наши эксперты помогли обнаружить фишинговые атаки и другую мошенническую активность. Компания передавала Интерполу аналитические данные о киберугрозах в рамках проекта [Stadia](#), инициативы Интерпола по обеспечению безопасности крупных международных мероприятий.
- Гран-при Сингапура в рамках этапа чемпионата мира «Формулы-1» 2025 года — мы предоставляли данные о киберугрозах, чтобы защитить участников от цифровых рисков.

Помимо Интерпола и Африпола, в число наших партнеров в борьбе с киберпреступностью входят:

- альянс [No More Ransom](#) (совместно с Европолом) — за девять лет работы помог более чем 6 млн пользователей восстановить свои данные без выплаты выкупа;
- Коалиция против стalkerского ПО (Coalition Against Stalkerware);
- Женевский диалог (Geneva Dialogue);
- Парижский призыв к доверию и безопасности в киберпространстве (Paris Call for Trust and Security in Cyberspace);
- Совет Европы;
- World Internet Conference (член Экспертно-консультативного комитета высокого уровня);
- Международный союз электросвязи;
- Международная организация по стандартизации (ISO);
- международный альянс Smart Africa и многие другие организации.



В 2025 году Компания стала членом Сектора развития электросвязи Международного союза электросвязи (ITU-D) и активно участвовала в глобальных форумах по кибербезопасности.

Проводим исследования целевых атак и продвинутой угрозы

По данным [отчета](#) от экспертов центра сервисов по кибербезопасности «Лаборатории Касперского», в 2025 году доля сложных целевых атак (APT) составила почти 24%. С подобной угрозой столкнулись около 21% компаний, использующих сервис Kaspersky MDR.

При этом их число существенно выросло —

на **74%**

по сравнению с 2023 годом

Также злоумышленники активно эксплуатируют социальную инженерию (15%), такая активность затронула 18% предприятий.

В 2025 году мы [выявили](#) и помогли устранить критическую уязвимость нулевого дня в Google Chrome (CVE-2025-2783), использовавшуюся в операции «Форумный Тролль», которая представляла собой серию сложных кибератак против российских организаций. В ходе исследования эксперты нашего Глобального центра исследований и анализа угроз (Kaspersky GReAT) впервые обнаружили использование шпионского ПО, созданного итальянской компанией Memento Labs (ранее HackingTeam), в реальных атаках.

Кроме того, эксперты Kaspersky GReAT [обнаружили](#) новую кампанию кибершпионажа PassiveNeuron, нацеленную на системы Windows Server в государственных, финансовых и промышленных организациях Азии, Африки и Латинской Америки (с декабря 2024 по август 2025 года).

Основные тренды в области киберугроз

Фишинговые и спам-кампании

В 2024–2025 годах в мире было заблокировано более 1,4 млрд переходов по фишинговым и скам-ссылкам. Злоумышленники активно создают поддельные страницы крупных брендов для кражи учетных данных и денег пользователей.

Угрозы в финансовом секторе и сложные атаки

В 2025 году финансовый сектор сталкивался с многоуровневыми угрозами: банковские троянцы, атаки через мессенджеры, атаки на цепочки поставок. Число кибератак на финансовые организации в России выросло на 43% по сравнению с годом ранее. Большинство (83%) финансовых учреждений столкнулись с киберугрозами в корпоративной электронной почте.

Рост активности финансово мотивированных злоумышленников

В 2025 году количество уникальных пользователей в финансовом секторе во всем мире, столкнувшихся с программами-вымогателями, возросло на 35,7% по сравнению с 2023 годом¹.

Автоматизация атак и использование ИИ

Злоумышленники активно используют машинное обучение и автоматизацию для более эффективного распространения вредоносного ПО и в попытке избежать обнаружения защитными решениями.

Угрозы для мобильных устройств

По данным Компании за 2025 год, число обнаруженных на Android мобильных угроз выросло почти в полтора раза. В третьем квартале их было на 38% больше, чем во втором.

Атаки на цепочки поставок

Кибератаки на цепочки поставок программного обеспечения стали самой частой угрозой для бизнеса в 2025 году. С ними столкнулись 31% компаний по всему миру, в России — 35%.

Помогаем развивать законодательство

Обладая обширными экспертными знаниями в области защиты критической инфраструктуры, борьбы с киберпреступностью и защиты данных, мы постоянно участвуем в рабочих группах и общественных консультациях по разработке международных и национальных нормативных документов, направленных на обеспечение кибербезопасности в мире.

«Лаборатория Касперского» активно участвовала в формировании Конвенции ООН против киберпреступности — первого в истории универсального международного договора в области информационной безопасности, принятого в декабре 2024 года. В октябре 2025 года Евгений Касперский выступил на панельной дискуссии по вопросам глобального сотрудничества для реализации программ по наращиванию потенциала в кибербезопасности, проходившей в рамках церемонии подписания конвенции в Ханое.

Мы также представили свои предложения при обсуждении Глобального цифрового договора ООН (принят в сентябре 2024 года), акцентируя внимание на вопросах повышения цифровой грамотности, подготовки специалистов, безопасности использования ИИ и противодействия стелс-активности.

Участвуем в разработке стандартов

«Лаборатория Касперского» вносит вклад в развитие международных и национальных стандартов в области кибербезопасности и безопасной разработки цифровых решений.

В отчетном периоде при участии экспертов Компании были разработаны новые стандарты:

- Международный стандарт ISO для устройств интернета вещей. Он описывает ключевые факторы благонадежности устройств интернета вещей и доверия к ним, а также формирует основу для более безопасного и устойчивого развития IoT-экосистем;
- Государственный стандарт по конструктивной безопасности, который вступил в силу 1 декабря 2025 года, — ГОСТ «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки». Стандарт определяет основные понятия и принципы конструктивной безопасности (Secure-by-Design) и утверждает приоритет такого подхода при разработке ПО и систем.

¹ Данные за период с ноября 2024 по октябрь 2025 года по сравнению с ноябрем 2022 — октябрём 2023 года.

Делимся экспертизой

Мы охотно делимся экспертизой в сфере кибер-безопасности, выступая на крупных мероприя-тиях и организуя собственные конференции, такие как Security Analyst Summit, с участием представите-лей правоохранных органов, государственных структур и академического сообщества. Публикуем информацию о киберугрозах в собственном [блоге](#) и на [портале](#), проводим бесплатные [вебинары](#) по кибербезопасности.

В 2024–2025 годах наши эксперты участвовали в многочисленных форумах и конференциях по кибер-безопасности, в число которых вошли:

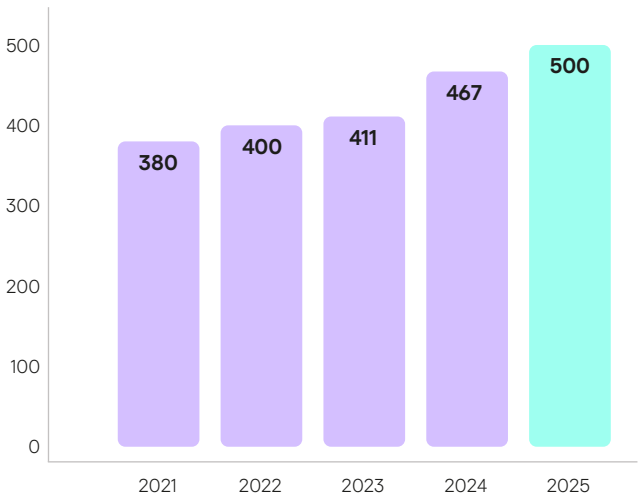
- рабочая группа открытого состава ООН по ИКТ (в рамках неформального диалога под эгидой пред-седателя рабочей группы);
- консультации Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступ-ных целях;
- Форум ООН по управлению интернетом;
- Глобальный цифровой договор ООН;
- Африканский форум по кибербезопасности;
- рабочие группы «Женевского диалога»;
- экспертные рабочие группы Интерпола;
- Всемирная конференция по вопросам интернета (Китай);
- Cyber Security Summit (Тяньцзинь, Китай);
- it-sa Expo&Congress (Германия);
- ЦИПР (Россия);
- Singapore International Cyber Week (Сингапур).

С ноября 2025 по март 2026 года эксперты Компании провели онлайн-тренинг «Мониторинг ИБ и поиск угроз» (Security operations and threat hunting) для порядка 40 представителей правоохранных органов из 23 государств — членов Африпола.

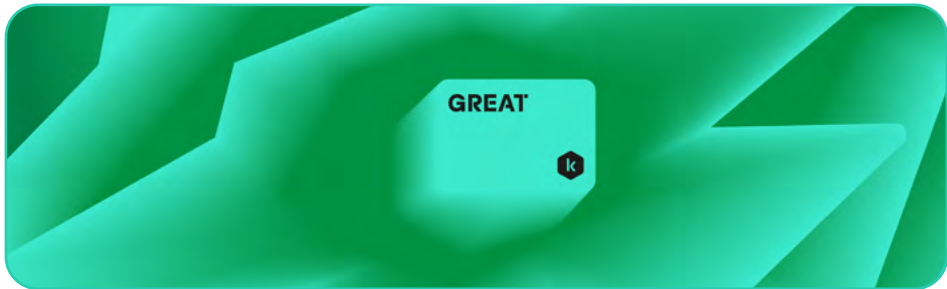
Итоги работы по направлению борьбы с киберзлоумышленниками

В 2025 году системы обнаружения киберугроз «Лаборатории Касперского» выявляли в среднем 500 000 вредоносных файлов в день — на 7% больше, чем в 2024 году¹.

Количество вредоносных файлов, обнаруживаемых «Лабораторией Касперского» ежедневно, тысяч штук



¹ См. отчет [Kaspersky Security Bulletin 2025](#). Статистика в отчете охватывает период с ноября 2024 по октябрь 2025 года.



- Наши эксперты обнаружили новую волну сложных целевых атак группы [Librarian Likho](#). Кампания нача-лась в декабре 2024 года и была активна на про-тяжении многих месяцев. Атаки проводились преимущественно с часа ночи до пяти часов утра по местному времени — в это время злоумышлен-ники пытались получить удаленный доступ к ком-пьютеру цели, украсть учетные данные и установить майнеры для нелегитимной добычи криптовалюты.
- Сотни российских корпоративных пользователей стали жертвами атак, также пострадали компании из Беларуси и Казахстана.
- В сентябре 2025 года мы выявили новую волну кибератак группы [Librarian Likho](#), направленную на российскую авиа- и радиопромышленность. Впервые злоумышленники использовали собствен-ное вредоносное ПО, разработанное с примене-нием искусственного интеллекта.
- Группа [Angry Likho](#) проводит атаки с января 2025 года, нацеливаясь на сотрудников корпо-раций России и Беларуси. В арсенале — стилеры для кражи конфиденциальных данных и утилиты удаленного администрирования для полного кон-троля над зараженным устройством.
- В 2025 году эксперты Kaspersky GReAT [раскрыли](#) схему, в которой злоумышленники украли у рос-сийского разработчика криптовалюту на сумму около \$500 000 через зараженный пакет с откры-тым исходным кодом. Он мимикрировал под рас-ширение для Cursor AI, среды разработки с поддержкой ИИ.

Наши планы на 2026 год

- Участие в формировании правового поля по борьбе с киберпреступностью
- Обучение и повышение квалификации экспертов, проведение тренингов по актуальным темам в области кибербезопасности
- Сотрудничество с внешними организациями и установление партнерских отношений с государственными учреждениями для обмена информацией о киберугрозах
- Регулярное обновление ПО и технологий для надежной защиты от киберугроз