

Как мы превращаем знания в защиту

GRI 3-3

Инвестируя в R&D и создавая инновационные технологии, мы превращаем знания и экспертизу в новые практические решения для защиты цифрового мира.

Инвестируем в исследования и новые продукты

~3 000

сотрудников Компании работают в области R&D

373

уникальные научные публикации
за 2024–2025 годы

Мы уверены: чтобы эффективно защищать людей и бизнес от киберугроз, нужно постоянно развиваться и быть на шаг впереди злоумышленников. Поэтому исследования и совершенствование защитных решений — одно из ключевых направлений работы «Лаборатории Касперского».

В R&D-подразделениях Компании работают порядка 3 000 специалистов — инженеры, аналитики, исследователи и разработчики. Их общая задача — превращать экспертизу и знания о киберугрозах в практические решения защиты, которые помогают клиентам чувствовать себя увереннее в цифровой среде.

За 2024–2025 годы наши эксперты подготовили 373 уникальные научные и аналитические публикации. В них мы делимся результатами исследований, наблюдениями о новых угрозах, подходами к защите и практиками, которые помогают рынку и сообществу лучше понимать, как устроен современный ландшафт киберрисков.



Основные направления разработок

В отчетном периоде «Лаборатория Касперского» в основном инвестировала в развитие трех новых и наиболее перспективных направлений:

- разработка и вывод на рынок нового продукта — межсетевого экрана нового поколения (NGFW);
- развитие и продажу Kaspersky Container Security;
- создание облачных продуктов для международного рынка (XDR Optimum, Cloud XDR).

Компания также разрабатывает инновационные решения на стыке кибер- и физической безопасности промышленных объектов. Например, система [Kaspersky Antidrone](#) предназначена для обнаружения беспилотников и защиты от них.

У проекта Kaspersky Antidrone четыре патента в России, два патента в США, три патента в Европе. Система отмечена премией AGBA в области инноваций в кибербезопасности и премией «Промышленный дизайн».



Расширяем защиту корпоративных сетей с помощью NGFW

Мы разработали и вывели на рынок межсетевой экран нового поколения (NGFW), созданный на базе глобальной экспертизы и передовых технологий Компании.

Это решение помогает бизнесу:

- защищать корпоративную сеть от широкого спектра киберугроз;
- контролировать активность приложений и сервисов;
- эффективно управлять трафиком, чтобы сеть работала стабильнее;
- оптимизировать производительность инфраструктуры, снижая риски простоев и инцидентов.

Делаем контейнерные и облачные среды безопаснее с Kaspersky Container Security

Kaspersky Container Security (KCS) — решение, которое обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла, от разработки до эксплуатации.

KCS помогает организациям:

- защитить бизнес-процессы и снизить вероятность инцидентов;
- соответствовать стандартам и нормам безопасности;
- встраивать безопасность в разработку и следовать принципу DevSecOps, когда защита внедряется с самого начала, на всех этапах жизненного цикла продукта;
- высвободить ресурсы ИБ-службы для других задач за счет автоматизации части проверок и контроля;
- сократить время вывода продуктов на рынок благодаря тому, что разработка и выпуск идут быстрее при сохранении необходимых требований к безопасности.

Kaspersky Container Security спроектирован с учетом особенностей контейнерных сред и обеспечивает защиту на разных уровнях: от образов контейнеров до операционной системы хоста — среды, на которой контейнеры работают.

KCS является частью комплексного решения по защите облачных рабочих нагрузок [Kaspersky Cloud Workload Security](#). В составе этой платформы оно помогает надежно защищаться от кибератак, сокращать время обнаружения угроз и реагирования на них в облачных средах.



Упрощаем выявление сложных атак с облачными XDR-продуктами

Мы создаем облачные продукты XDR для международного рынка — XDR Optimum и Cloud XDR, — чтобы компаниям было проще находить и останавливать сложные кибератаки.

XDR — это концепция в информационной безопасности, которая помогает:

- проактивно выявлять угрозы сразу на разных уровнях инфраструктуры;
- быстро реагировать на инциденты;
- противодействовать сложным атакам, которые не всегда заметны по одному признаку.

XDR объединяет возможности EDR (защиты конечных устройств) с другими инструментами безопасности максимально от одного производителя, а также подключает дополнительные источники данных. В итоге специалисты получают:

- единую точку принятия решения;
- удобный интерфейс;
- расширенные возможности для расследования сложных киберинцидентов.

Для международного рынка мы создаем этот продукт в облачной поставке — такой формат помогает компаниям существенно оптимизировать стоимость использования решения и быстрее получать нужный эффект без усложнения инфраструктуры.