

Масштабируем безопасность, объединяя знания и опыт

GRI 3-3

Наша цель — защищать пользователей и организации от киберугроз с помощью передовых технологий, накопленной экспертизы и инициатив.

Решения «Лаборатории Касперского»

>14 млн

атак с использованием вредоносного, рекламного или нежелательного мобильного ПО предотвратили в 2025 году

>144 млн

вредоносных почтовых вложений заблокировали в 2025 году

Обнаружили и заблокировали веб-угрозы¹ на устройствах

34%

пользователей в России в 2025 году (27% — в мире)

Обнаружили локальные угрозы (on-device threats)² на устройствах

37%

пользователей в России (33% — в мире)

Противостояние современным киберугрозам в «Лаборатории Касперского» начинается с анализа того, как устроен современный цифровой мир, какие угрозы в нем возникают и как они меняются. Поэтому в основе всей нашей деятельности в этой области лежит работа центров экспертизы — команд разнопрофильных специалистов, которыми мы по-настоящему гордимся.

Они объединяют исследователей, аналитиков, инженеров и практиков, которые ежедневно изучают киберугрозы, исследуют кибератаки, разрабатывают новые технологии защиты и помогают организациям по всему миру справляться с инцидентами.



¹ Веб-угрозы — киберугрозы, которые проникают на устройства через интернет.

² Речь идет о киберугрозах, которые распространяются через съемные USB-накопители, CD и DVD либо изначально попадают на компьютер в завуалированном виде, например в составе файлов-установщиков и в зашифрованных файлах.

Пять центров экспертизы «Лаборатории Касперского»



1. Kaspersky Global Research and Analysis Team (GReAT)

Глобальный центр исследований и анализа угроз — команда экспертов, стратегически распределенная по всему миру. Она исследует наиболее сложные [APT-атаки](#), кампании кибершпионажа и деятельность организованных кибергрупп. Специалисты GReAT отслеживают деятельность более 900 групп и операций по всему миру, изучают тактики, методы и инструменты.

Результаты этих исследований становятся основой для совершенствования механизмов защиты от продвинутых угроз, а также для эксклюзивных отчетов об [APT-угрозах](#) и об [угрозах, связанных с финансово мотивированными атаками](#). Эти знания используются экспертами других центров «Лаборатории Касперского», а также нашими клиентами по всему миру для построения собственных систем кибербезопасности.

О самых резонансных расследованиях специалисты GReAT рассказывают в [подкасте](#) «Кибер Трукрайм».



2. Kaspersky Threat Research

Центр исследования киберугроз фокусируется на повседневной, но не менее важной работе — глубоком анализе тактик, техник и подходов злоумышленников. Эксперты центра исследуют вредоносное и нежелательное программное обеспечение, фишинг, спам и другие угрозы, связанные с онлайн-коммуникацией.

Отдельное направление посвящено безопасности программного обеспечения: снижению рисков появления уязвимостей, развитию жизненного цикла безопасной разработки, безопасности кибериммунных продуктов и решений Компании, созданных на основе нашей собственной операционной системы KasperskyOS.

Благодаря работе Threat Research защитные технологии «Лаборатории Касперского» способны выявлять и блокировать даже самые новые и быстро меняющиеся киберугрозы.



3. Kaspersky AI Technology Research

Центр исследования технологий искусственного интеллекта — один из самых многогранных в нашей экспертизе. Он объединяет специалистов, которые изучают, разрабатывают и внедряют технологии на базе ИИ для задач кибербезопасности. Алгоритмы машинного обучения и средства аналитики на основе генеративного ИИ используются для обнаружения и приоритизации угроз, анализа больших массивов данных и автоматизации рутинных процессов. Они помогают в исследовании особенно запутанных случаев и самых сложных угроз.

Эти технологии используются как для защиты частных пользователей, так и в сложных корпоративных и промышленных средах. Среди решений центра — [Kaspersky Machine Learning for Anomaly Detection](#) (MLAD) для выявления аномалий в производственных процессах.

Кроме того, эксперты центра исследуют уязвимости систем на базе ИИ и изучают способы, с помощью которых искусственный интеллект может применяться злоумышленниками, чтобы в дальнейшем совершенствовать защиту для пользователей.



4. Kaspersky Security Services

Центр сервисов по кибербезопасности оказывает экспертную поддержку клиентам по всему миру — от экстренного реагирования на инциденты до оценки уязвимостей и сопровождения создания центров мониторинга безопасности (SOC — Security Operations Center).

Центр сервисов по кибербезопасности — это практическая экспертиза «в поле». Специалисты центра работают

с ИБ-командами крупнейших организаций мира, помогая им бороться с инцидентами, анализировать выявленные атаки и предотвращать новые, предоставляя широкую линейку экспертных сервисов.

Отслеживание подозрительной активности и экстренное реагирование на инциденты ([Managed Detection and Response](#), MDR), оценка защищенности, консалтинг по созданию собственного SOC-центра и выявление угрозы данным — все эти сервисы основаны на реальном опыте борьбы с кибератаками и тесно связаны с исследованиями других центров.



5. Kaspersky ICS CERT

Центр исследования безопасности промышленных систем ([Kaspersky ICS CERT](#)) был создан для противодействия характерным для АСУ ТП киберугрозам. Эксперты центра выявляют уязвимости в чувствительных к сбоям средах и принимают участие в деятельности международных промышленных ассоциаций в качестве экспертов и аналитиков.

Результаты этих исследований становятся базой для сервисов промышленной аналитики угроз — Industrial (ICS) Threat Intelligence¹, которые доступны через платформу [TIP](#)². Это [отчеты](#) о результатах исследований, машиночитаемые потоки [индикаторов компрометации](#) (IoC) и [данных об уязвимостях](#).

Отдельное важное направление деятельности ICS CERT — помощь производителям программно-аппаратных продуктов. Центр помогает проверить уровень зрелости кибербезопасности их решений и сделать эти решения более безопасными.

¹ Специализированная аналитика киберугроз, ориентированная на промышленные системы и объекты критической инфраструктуры.

² TIP (Threat Intelligence Platform) — платформа для работы с аналитикой угроз.