Масштабируем безопасность

Отчет об устойчивом развитии
«Лаборатории Касперского»
за 2024-2025 годы

kaspersky.ru

kaspersky

Содержание

Обращение Генерального директора

GRI 2-22

Дорогие друзья!

С каждым годом цифровая среда становится все сложнее, угрозы — разнообразнее, а зависимость людей, бизнеса и государств от технологий — глубже. В этих условиях для нас особенно важно отвечать на новые вызовы и расширять возможности для безопасного развития цифрового мира. Подход, который лежит в основе нашей работы, остается неизменным: максимальную безопасность может обеспечить только кибериммунитет.

Уже почти три десятилетия «Лаборатория Касперского» развивает технологии информационной безопасности, помогая людям и организациям пользоваться преимуществами цифровизации и развиваться без лишних рисков.

Компания продолжает расти, усиливать экспертизу и расширять международное присутствие: сегодня мы защищаем пользователей более чем в 200 странах. В августе 2024 года начал работу наш офис в Боготе — третий в Латинской Америке, а в конце 2025 года мы усилили присутствие в Юго-Восточной Азии, открыв новое представительство во Вьетнаме. В отчетном периоде также открылись новые Центры прозрачности в Турции, Южной Корее и Колумбии. Эти шаги для нас означают, что больше клиентов в разных странах получают прямой доступ к нашей экспертизе, технологиям и принципам открытости.

За этим ростом стоит не только масштаб бизнеса, но и масштаб ответственности: чем шире географическое присутствие и количество клиентов, полагающихся на наши технологии, тем выше требования к надежности, прозрачности и качеству защиты. Базой для этого остаются наши технологии, международная экспертиза и постоянная готовность пересматривать подходы в ответ на меняющийся ландшафт угроз.

Наша продуктовая линейка развивается вместе с потребностями цифрового мира. На конец 2025 года она насчитывала уже 43 продукта. Мы последовательно расширяем экосистему решений для дома и бизнеса, для промышленных предприятий и критической инфраструктуры, для организаций, которым нужна системная устойчивость к самым разным угрозам.

Особое внимание мы уделяем развитию кадрового потенциала отрасли. Мы продолжаем вкладываться в цифровое просвещение, работу со школьниками, студентами, молодыми и действующими специалистами. «Лаборатория Касперского» взаимодействует примерно с 200 вузами в 45 государствах, включая более 70 учебных заведений в России и странах СНГ. Это часть нашего долгосрочного вклада в устойчивость всей отрасли: сильная цифровая среда начинается с сильных специалистов, способных проектировать, внедрять и защищать технологии будущего.

В последние годы новым вызовом и в то же время возможностью для нашего мира стал искусственный интеллект, его ответственное развитие и применение. Мы давно используем такие технологии в собственных продуктах и исследованиях, но сегодня принципиально важно не только наращивать их возможности, но и формировать правила безопасного использования. В декабре 2024 года на Форуме Организации Объединенных Наций по управлению интернетом в Эр-Рияде мы представили руководство по безопасной разработке и внедрению систем искусственного интеллекта. Его цель — помочь организациям учитывать киберриски, связанные с применением таких технологий, и снижать их еще на этапе проектирования и внедрения. Также «Лаборатория Касперского» стала участником российского Альянса в сфере искусственного интеллекта, поддерживающего ответственное развитие технологий, и присоединилась к глобальному альянсу Организации Объединенных Наций по промышленному развитию в области искусственного интеллекта для промышленности и производства.

Но устойчивое развитие для нас по-прежнему шире технологической повестки. Мы продолжаем развивать все ключевые направления нашей стратегии: укреплять киберустойчивость, инвестировать в инновации, совершенствовать практики прозрачности и деловой этики, снижать собственное воздействие на окружающую среду, поддерживать сотрудников и вносить вклад в развитие общества.

Сегодня для нас очевидно, что безопасность нельзя считать раз и навсегда достигнутым состоянием. Ее нужно развивать, усиливать, делать доступной для разных отраслей, регионов и пользователей. Именно так мы понимаем свою миссию — шаг за шагом расширять пространство, в котором люди и организации могут уверенно пользоваться цифровыми технологиями, расти и строить будущее.

От имени Компании я хочу поблагодарить наших сотрудников, партнеров, клиентов и всех, кто разделяет наши ценности, за доверие, профессионализм и готовность двигаться вперед вместе с нами. Уверен, что, только объединяя экспертизу, ответственность и открытость, мы сможем сделать цифровой мир по-настоящему безопасным и устойчивым для всех.

Евгений Касперский
Генеральный директор
«Лаборатории Касперского»

О Компании

«Лаборатория Касперского» — международная компания, которая разрабатывает инновационные решения в области кибербезопасности, защиты данных и цифровой приватности. Мы стремимся сделать цифровое пространство безопасным для каждого и построить будущее, в котором технологии работают на благо человечества.

>1 млрд

устройств[1] более чем в 200 странах и территориях защищено от массовых киберугроз и целенаправленных атак

>2 млрд угроз

обнаружено с момента создания Компании

~200 тысяч

корпоративных клиентов

[1] Согласно данным Kaspersky Security Network (KSN) по автоматизированному анализу вредоносных программ, включающим информацию с 2011 года.

Главное о «Лаборатории Касперского»

На фоне повсеместного перехода к цифровой модели экономики кибербезопасность стала базовой потребностью глобального устойчивого развития. С 1997 года «Лаборатория Касперского» работает над тем, чтобы масштабировать надежную защиту, делая ее доступной каждому.

Защитные решения Компании используются в

>200

странах и территориях

~5,7 тысячи

сотрудников в команде

43

продукта в портфеле

5

центров экспертизы

Миссия и ценности

Миссия «Лаборатории Касперского» — строить безопасный и устойчивый цифровой мир, в котором технологии помогают улучшать жизнь на планете.

Мы реализуем свою миссию через три ключевых направления:

- **повышение устойчивости цифрового пространства, в том числе путем развития кибериммунитета и разработки изначально защищенных систем;**
- **содействие социальному развитию и благополучию общества;**
- **защиту окружающей среды и ресурсов планеты.**

Подробнее о кибериммунитете — на с. 37

Слушать и слышать

Наши клиенты, партнеры и команда всегда в фокусе нашего внимания. В своих решениях мы опираемся на их задачи и прислушиваемся к их потребностям. Мы обеспечиваем уровень безопасности, соответствующий самым высоким требованиям. Люди, для которых мы работаем, чувствуют нашу поддержку в любой ситуации и знают, что выбирают лучшую защиту, которая создана именно для них.

Подтверждать лидерство

Мы ежедневно укрепляем свой лидерский статус, создавая передовые технологии, которые делают мир безопаснее. Мы никогда не перестаем работать над собой и развивать свою экспертизу. В области кибербезопасности нам нет равных: это подтверждают независимые эксперты индустрии. Клиенты, партнеры и пользователи доверяют нам. Мы, в свою очередь, считаем своим профессиональным долгом оправдывать это доверие и оставаться честными перед ними и перед самими собой.

Превосходить себя каждый день

Мы постоянно думаем, как сделать свои продукты еще лучше, и стремимся превзойти свои достижения, внедряя новые технологии и предугадывая новые угрозы.

Мы настойчиво испытываем на прочность собственные разработки и всегда находим способы еще на шаг приблизиться к совершенству. Мы никогда не стоим на месте и постоянно развиваемся, сохраняя свои ценности. Именно это раз за разом выводит эффективность наших решений на новый уровень.

Быть сильнее трудностей

Как бы много и часто нам ни бросали вызов, мы становимся только сильнее. Мы делаем то, чего не могут другие, и решаемся на то, чего не делали раньше сами. Выделяемся, диктуем свои правила и гордимся тем, что отличает нас от остальных. Мы не ищем легких путей и простых задач, потому что умеем превращать трудности в возможности. Мы находим нестандартные решения даже в сложных ситуациях и делаем это по-своему.

География

GRI 2-1

Продукты «Лаборатории Касперского» используются нашими клиентами по всему миру. Группа компаний «Лаборатория Касперского» работает более чем в 30 странах и территориях на пяти континентах. Решения Компании защищают пользователей более чем в 200 странах и территориях.

В каких странах и территориях работают компании «Лаборатории Касперского»

СНГ

- Беларусь
- Казахстан
- Россия

Ближний Восток, Турция и Африка

- Израиль
- Руанда
- Саудовская Аравия
- Турция
- ОАЭ
- ЮАР

Латинская Америка

- Бразилия
- Колумбия
- Мексика

Европа

- Великобритания
- Германия
- Испания
- Италия
- Нидерланды
- Португалия
- Франция
- Чехия
- Швейцария

Азиатско-Тихоокеанский регион

- Австралия
- Вьетнам
- Индия
- Китай и Гонконг
- Малайзия
- Сингапур
- Южная Корея
- Япония

Северная Америка

- Канада

Бизнес-модель

GRI 2-6

Мировой рынок ИБ[1]

B2B

$83,3 млрд
размер глобального B2B-рынка ИБ в 2025 году

$136 млрд
прогноз глобального B2B-рынка ИБ в 2029 году

+13%
среднегодовой темп роста B2B-рынка

B2C

$6,3 млрд
размер глобального B2C-рынка ИБ в 2025 году

$7,6 млрд
прогноз глобального B2C-рынка ИБ в 2029 году

+5%
среднегодовой темп роста B2C-рынка

kaspersky

$836 млн
выручка в 2025 году

+4%
год к году — рост в 2025 году

Направления бизнеса и продуктовая линейка B2B

Защита конечных устройств
EDR Expert, Small Office Security, Mobile Security

Безопасность облачных и виртуальных сред
Cloud Workload Protection (включая Hybrid Cloud, Container Security), Security for storage, Scan Engine

Безопасность сетей и электронной почты
NDR (Anti Targeted Attack), Mail Security Gateway, Security for Office 365 / MS Exchange, NGFW, SD-WAN, Anti-DDoS, Web Traffic Security

Единая ИБ-платформа (Security Operations) Open Single Management Platform

Платформа для обнаружения и реагирования на сложные угрозы
Symphony XDR

Мониторинг и управление событиями ИБ
SIEM (Unified Monitoring and Analysis Platform)

Платформа и сервисы киберразведки
Threat Intelligence

AI-ассистент

Промышленная кибербезопасность
Industrial CyberSecurity — native OT XDR platform (nodes, networks)

Сервисы ИБ
MDR, Incident response, Security Assessment, Premium support и Professional services и др.

Тренинги ИБ
Automated Security Awareness Platform, тренинги по кибербезопасности и др.

Операционная система Решения на базе Kaspersky OS: Thin Client, OS Mobile, Automotive Secure Gateway

Направления бизнеса и продуктовая линейка B2C

Основное предложение

Трехуровневое предложение
- Kaspersky Standard
- Kaspersky Plus
- Kaspersky Premium

Отдельные приложения
- Kaspersky Secure Connection
- Менеджер паролей: Kaspersky Password manager
- Защита от спам-звонков: Kaspersky Who Calls[2]
- Родительский контроль: Kaspersky Safe Kids
- Геотрекинг: K-tag/PetKa
- eSIM-сервис: Kaspersky eSIM Store

Партнерские предложения в рамках отношений с поставщиками услуг и реселлерами
- Kaspersky Safe Web (Web-based)
- Kaspersky Smart Home (Router-based)

Каналы продаж B2B

- Партнерская сеть: дистрибьюторы, реселлеры, системные интеграторы, сервис-провайдеры (MSP), провайдеры управляемых служб безопасности (MSSP) и пр.
- Технологические альянсы (интеграции с продуктами партнеров)
- Цифровой канал продаж

Каналы продаж B2C

- Прямые продажи пользователям через интернет / цифровой канал
- Розничные каналы продаж (магазины, реселлеры)
- Партнеры: провайдеры интернета, мобильные операторы, банки и пр., предлагающие защиту в комплекте со своими услугами

Продвижение

- Интегрированные рекламные кампании для продвижения бренда и решений (наружная реклама, цифровое продвижение, сотрудничество с сообществами, социальные сети, подкасты и PR)
- Совместный маркетинг с партнерами и коллаборации с другими брендами
- Участие в отраслевых и индустриальных конференциях и выставках
- Контент-маркетинг и аналитика угроз (исследования GReAT), публикации, блоги, вебинары
- Повышение доверия через Центры прозрачности, программы Bug Bounty, международные конференции SAS (Security Analyst Summit) и пр.
- Участие в социальных проектах для развития культуры безопасности и кибергигиены
- Вовлечение школьников и студентов в индустрию IT/ИБ

Клиенты по всему миру

~1 млрд
устройств под защитой решений «Лаборатории Касперского»

~200 тысяч
корпоративных клиентов по всему миру выбирают нашу защиту

- Государственный сектор
- Крупные предприятия
- Промышленные компании
- Малые и средние предприятия
- Частные пользователи ПК и смартфонов

[1] Оценка рынка выполнена по внутренней методологии Компании. В оценку включены только сегменты ИБ, в которых Компания ведет деятельность.

[2] WhoCalls доступен в России, Казахстане, Индонезии и Латинской Америке.

Продукты

Решения «Лаборатории Касперского» обеспечивают надежную защиту от киберугроз для частных пользователей, малых компаний и крупнейших корпораций, год за годом завоевывая признание ведущих независимых экспертов.

GRI 2-6

В портфеле Компании — 43 продукта информационной безопасности для дома и бизнеса[1]. В 2013–2025 годах решения «Лаборатории Касперского» приняли участие в 1 122 независимых тестированиях и обзорах. Они оценивались несколькими независимыми организациями, включая AV-Comparatives, AV-TEST, SE Labs, и в 861 случае заняли первое место, а в 965 — вошли в тройку лучших. Топ-3 «Лаборатории Касперского» за этот период составил 86%.

В 2025 году продукты «Лаборатории Касперского»:

участвовали в 100 независимых тестированиях и обзорах

в 94 случаях вошли в тройку лучших

в 90 случаях заняли первое место

Решения для домашних пользователей

- Kaspersky Standard
- Kaspersky Plus
- Kaspersky Premium
- Kaspersky Safe Kids
- Kaspersky Secure Connection
- Kaspersky Who Calls
- Kaspersky Password Manager
- PetKa
- Kaspersky eSIM Store

Подробнее о продуктах для домашних пользователей

Решения на базе KasperskyOS

- KasperskyOS SDK для IoT-контроллеров
- Kaspersky Automotive Secure Gateway
- Kaspersky Thin Client

Подробнее о решениях на KasperskyOS

Основные решения для бизнеса

- Kaspersky Endpoint Security для бизнеса
- Kaspersky Symphony Security
- Kaspersky EDR
- Kaspersky XDR
- Kaspersky Industrial CyberSecurity
- Kaspersky MDR
- Kaspersky Anti-Targeted Attack Platform
- Kaspersky Automated Security Awareness Platform
- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky Threat Intelligence
- Kaspersky NGFW
- Kaspersky Digital Footprint Intelligence

Подробнее об этих и других решениях для бизнеса

43 продукта в портфеле Компании

[1] В перечень продуктов включены защитные решения, представленные на сайтах kaspersky.ru и kaspersky.com. Данные продукты предоставляются по большому количеству лицензий, удовлетворяющих потребностям различных клиентов (всего более 1 500 позиций в прайс-листе Компании).

Краткая история Компании

За почти 30 лет работы «Лаборатория Касперского» стала одним из лидеров развития технологий кибербезопасности, защищающих частных пользователей, бизнес, промышленность и государственные структуры в России и более чем в 200 странах и территориях мира.

1997

- Основание «Лаборатории Касперского»

1999

- Открытие первого зарубежного офиса — в Великобритании

2001

- Разработка антивирусного ПО для портативных устройств

2007

- Запуск линейки продуктов для бизнеса

2008

- Создание Kaspersky GReAT (глобального центра исследования и анализа угроз)

2013

- Начало сотрудничества с Интерполом

2015

- Выпуск специализированного решения для защиты критически важных инфраструктур и промышленных объектов

2016

- Участие в запуске проекта No More Ransom для помощи жертвам программ-вымогателей
- Открытие первого в России центра реагирования на компьютерные инциденты на индустриальных и критически важных объектах — Kaspersky ICS-CERT

2017

- Презентация собственной операционной системы

2018

- Запуск глобальной инициативы по информационной открытости (GTI)

2019

- Новый ребрендинг, сформулирована новая миссия Компании: «Строим безопасный мир»

2021

- Открытие доступа к Software Bill of Materials (SBOM), чтобы клиенты и партнеры понимали, что находится внутри продуктов и программного обеспечения «Лаборатории Касперского»
- Завершение сделки с Brain4Net, что способствовало дальнейшему развитию полномасштабной XDR-системы

2023

- Получение награды «Продукт года» от AV-Comparatives для решения Kaspersky Standard

2024

- Заключение договора о сотрудничестве с Африполом

2025

- Представление коммерческой версии Kaspersky NGFW
- Открытие новых направлений бизнеса — представлены Kaspersky eSIM Store и решение для поиска потерявшихся в городе питомцев (Kaspersky Tag — физическая Bluetooth-метка и PetKa — бесплатное приложение, с которым работает Kaspersky Tag)

Важнейшие события отчетного периода

Расширение бизнеса

- **Открытие трех новых Центров прозрачности в ключевых регионах.** «Лаборатория Касперского» в 2024 году продолжила расширение Глобальной инициативы по информационной открытости, начали работать Центры прозрачности в Турции, Южной Корее и Колумбии.
- **Расширение присутствия в Латинской Америке и Юго-Восточной Азии.** В августе 2024 года «Лаборатория Касперского» открыла офис в Боготе (Колумбия), который стал ее третьим представительством в Латинской Америке. А в ноябре 2025 года был открыт офис во Вьетнаме и назначен новый генеральный директор в Юго-Восточной Азии.

Инновации

- **Kaspersky NGFW.** В России представлен межсетевой экран нового поколения с показателем обнаружения и предотвращения угроз свыше 95%, собственным антивирусным движком на базе ИИ, отказоустойчивостью и производительностью до 180 Гб/с. Коммерческий запуск продукта состоялся в августе 2025 года.
- **Kaspersky Cloud Workload Security.** «Лаборатория Касперского» запустила комплексное решение для защиты облачных рабочих нагрузок, состоящее из Kaspersky Hybrid Cloud Security и Kaspersky Container Security. Совместная установка систем позволяет защитить инфраструктуру, где бы она ни находилась: на серверах, виртуальных машинах, в частных, общедоступных, гибридных облаках и др.
- **Интеграция GigaChat в SIEM-систему KUMA.** Добавлена возможность анализировать события безопасности с помощью нейросетевой модели GigaChat от Сбера. Новая функциональность получила название KIRA — Kaspersky Investigation and Response Assistant. Это решение повысит эффективность команды безопасности.
- **Kaspersky Thin Client 2.0.** Компания презентовала новую версию операционной системы на базе KasperskyOS с расширенными возможностями удаленного подключения, более быстрой загрузкой и запуском приложений, усовершенствованным интерфейсом и быстрой интеграцией.
- **Запуск новых потребительских решений.** В 2025 году Компания вышла на новые сегменты рынка, представив клиентам Kaspersky eSIM Store — приложение для подбора, покупки и подключения eSIM, действующее более чем в 150 странах, а также запустив решение для поиска потерявшихся домашних животных PetKa.

Стандарты и сертификаты

- **Новый международный стандарт ISO для устройств интернета вещей.** «Лаборатория Касперского» участвовала в разработке стандарта, который описывает факторы благонадежности устройств интернета вещей и доверия к ним. Он подготовлен совместно с Международной организацией по стандартизации (International Organization for Standardization, ISO) и Международной электротехнической комиссией (International Electrotechnical Commission, IEC).
- **Руководство по безопасной разработке ИИ.** На Международном форуме ООН по управлению интернетом в Эр-Рияде Компания представила руководство, цель которого — помочь организациям избежать киберрисков, связанных с применением технологий ИИ.
- **Новый государственный стандарт по конструктивной безопасности.** «Лаборатория Касперского» помогла разработать ГОСТ «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки». Он начал действовать с 1 декабря 2025 года.
- **Сертификат на разработку ПО для автопрома.** Компания первой в России получила сертификат ISO 26262 на процесс разработки ПО для автомобильной индустрии. Теперь «Лаборатория Касперского» может предлагать заказчикам программные продукты, соответствующие требованиям ASIL B[1], что открывает новые возможности сотрудничества с автопроизводителями и интеграторами.
- **Сертификат на безопасную разработку.** «Лаборатория Касперского» первой в России прошла сертификацию процессов безопасной разработки ПО и получила сертификат № 1 в ФСТЭК России о соответствии этих процессов требованиям ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Международное сотрудничество

- **Сотрудничество с Африполом.** «Лаборатория Касперского» заключила пятилетнее соглашение с Африполом о совместном противодействии киберугрозам на Африканском континенте.
- **Операция Serengeti с Интерполом и Африполом.** Компания приняла участие в операции, в результате которой были арестованы более тысячи подозреваемых в киберпреступлениях в странах Африки. Обезврежено свыше 134 тысяч объектов вредоносной инфраструктуры.
- **Участие в операции Интерпола Synergia II.** Компания помогла Интерполу в операции, направленной на борьбу с распространением вредоносного ПО и фишинговыми атаками по всему миру. В результате был арестован 41 человек.
- **Помощь Интерполу в борьбе с Grandoreiro.** «Лаборатория Касперского» оказала содействие Интерполу в задержании пяти администраторов вредоносного ПО Grandoreiro — банковского троянца, который причинил ущерб более чем на 3,5 млн евро.

Образование и социальная ответственность

- **Сотрудничество с Босфорским университетом.** Подписан меморандум о взаимопонимании для создания Лаборатории прозрачности и развития совместных программ обучения в области кибербезопасности и информационной открытости.
- **Сотрудничество с Физтех-школой прикладной математики и информатики (ФПМИ) МФТИ.** Подписано соглашение о разработке и развитии программ подготовки специалистов в сфере кибербезопасности и ИИ.
- **Присоединение к Альянсу в сфере ИИ.** Компания стала членом российского Альянса в сфере искусственного интеллекта, ориентированного на ответственное развитие ИИ-технологий.
- **Запуск обучающих курсов по безопасной работе в интернете.** Компания запустила на своей платформе Kaspersky Automated Security Awareness Platform курсы по безопасному обращению с нейросетями. Также запущены новые курсы в сфере кибербезопасности на сайте Kaspersky Academy, платформа Kaspersky Cybersecurity Training с онлайн-тренингами для IT- и ИБ-специалистов и ряд других проектов.

[1] Automotive Safety Integrity Level B — это средний уровень риска для автомобильных электронных систем, означающий, что система должна обеспечивать высокую надежность для предотвращения опасных отказов.

Награды и признание

Наши решения по-прежнему получают высокую оценку независимых экспертов и завоевывают награды в престижных международных тестированиях.

В период 2024-2025 годов можно выделить следующие достижения наших решений.

Kaspersky EDR Expert:

- показало 100%-ную эффективность против таргетированных атак в исследовании AV-Comparatives Endpoint Prevention and Response Test, заслужив высокие награды **Strategic Leader 2024** и **Certified 2025** (подводя итоги результатов за 2022–2025 годы, решение три раза подряд получило награду Strategic Leader и один раз — Certified после отмены тестером всех остальных градаций наград в 2025 году);
- первым в индустрии успешно прошло все испытания в исследовании AV-Comparatives EDR Detection Validation Certification Test 2025, заслужив награду **Certified EDR Detection 2025**;
- в исследованиях AV-TEST Advanced EDR Test показало высокие результаты обнаружения и классификации тактик и техник продвинутых атак и заслужило награду **Approved Advanced EDR 2024**.

Kaspersky Small Office Security заслужило:

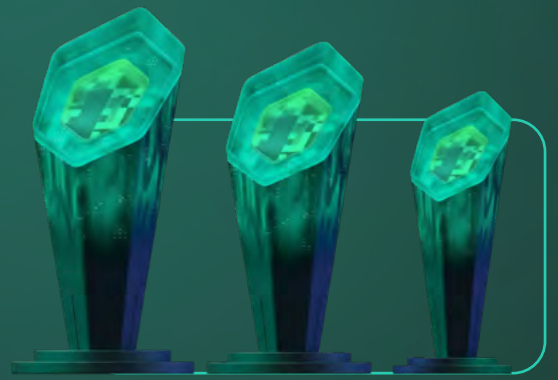
- годовую награду **AV-TEST BEST Protection 2024** за лучшие результаты во всех двухмесячных тестах 2024 года;
- годовые награды **AV-TEST BEST Advanced Protection 2024 + 2025** за абсолютные показатели в тестах защиты от сложных угроз в течение каждого года;
- годовые награды **AV-TEST Best Usability 2024 + 2025** за лучшую устойчивость к ложным срабатываниям в течение каждого года;
- годовую награду **SE Labs Winner Small Business Endpoint 2025** за высокие результаты в квартальных тестах, включая топ-1 результаты по параметру Total Accuracy Rating на протяжении III квартала 2023 года — III квартала 2025 года.

Kaspersky Endpoint Security заслужило:

- годовую награду **AV-TEST BEST Protection 2024** за лучшие результаты во всех двухмесячных тестах 2024 года;
- годовые награды **AV-TEST BEST Advanced Protection 2024 + 2025** за абсолютные показатели в тестах защиты от сложных угроз в течение каждого года;
- годовые награды **AV-TEST Best Usability 2024 + 2025** за лучшую устойчивость к ложным срабатываниям в течение каждого года;
- награду **Approved Anti-Tampering 2025**, успешно отразив все атаки на защитное решение на устойчивость к попыткам вмешательства в его работу в исследовании AV-Comparatives: Anti-Tampering Test 2025;
- награду **Approved Credential Dumping 2024**, успешно защитив от всех атак несанкционированного доступа к учетным данным в тесте AV-Comparatives: Credential Dumping test 2024;
- награду **Approved Process Injection 2024**, успешно защитив от 14 из 15 атак неавторизованного внедрения в процессы в тесте AV-Comparatives: Process Injection Test 2024;
- годовую награду **SE Labs Winner Enterprise Endpoint 2025** за высокие результаты в квартальных тестах, включая топ-1 результаты по параметру Total Accuracy Rating на протяжении III квартала 2023 года — III квартала 2025 года.

Решение Kaspersky Premium для защиты домашних пользователей заслужило:

- годовую награду **«Высокорейтинговый продукт (Top Rated)»** 2024 и 2025 годов от AV-Comparatives за высокие показатели в тестах в течение каждого года. Более того, продукт заслужил больше всех годовых наград от AV-Comparatives за все время проведения тестов с 2004 года;
- годовую награду **AV-TEST BEST Protection 2024** за лучшие результаты во всех двухмесячных тестах в течение года;
- годовые награды **AV-TEST Best Usability 2024 и 2025** за лучшую устойчивость к ложным срабатываниям в течение каждого года;
- годовые награды **AV-TEST BEST MacOS Security 2024 + 2025** за высокие показатели в квартальных тестах в течение каждого года;
- годовую награду **SE Labs Winner Consumer Endpoint 2025** за высокие результаты в квартальных тестах, включая топ-1 результаты по параметру Total Accuracy Rating на протяжении III квартала 2023 года — III квартала 2025 года;
- годовую награду **SE Labs Best Home Anti-Malware 2024** за высокие результаты в квартальных тестах;
- награду **Approved Fake Shops Detection 2025** от AV-Comparatives;
- награду **Approved Anti-Phishing 2024** от AV-Comparatives, получив первое место по результатам AV-Comparatives: Anti-Phishing Certification 2024.



Kaspersky Secure Connection:

- в 2024 году решения Kaspersky Premium и Kaspersky Secure Connection успешно прошли все испытания в исследовании AV-TEST и получили сертификаты **AV-TEST Approved VPN 2024**;
- в 2025 году решения Kaspersky Premium и Kaspersky Secure Connection уверенно обошли остальные восемь решений конкурентов по параметру Combined Score Ranking и получили сертификаты **AV-TEST Approved VPN 2025.**

Kaspersky Safe Kids (KSK):

- в 2024 году KSK показало высокий уровень детектирования и нулевой уровень ложных срабатываний и стало единственным среди пяти протестированных решений, которое выполнило критерии сертификации и получило статус **Approved Parental Control 2024** от AV-Comparatives;
- в 2025 году KSK вновь показало наивысший среди всех участников уровень детектирования и нулевой уровень ложных срабатываний, выполнив критерии сертификации и получив **Approved Parental Control 2025** от AV-Comparatives.

2024

- Всего в 2024 году продукты «Лаборатории Касперского» приняли участие в 95 независимых тестах и обзорах, 91 раз заняли первые места и 92 раза вошли в тройку лидеров. Общая доля вхождений в топ-3 достигла рекордных 97%.
- Решения «Лаборатории Касперского» для бизнеса, Kaspersky Small Office Security и Kaspersky Plus получили наивысшие оценки по результатам теста SE Labs. Они показали 100%-ную эффективность против киберугроз по итогам всех четырех тестов.
- «Лаборатория Касперского» вновь стала лидером на глобальном рынке управляемых решений по версии Quadrant Knowledge Solutions.
- Решение Kaspersky Standard по итогам тестов AV-Comparatives показало один из лучших результатов, суммарно получив 100 баллов из 105 возможных.
- «Лаборатория Касперского» получила девять наград BEST 2024 от AV-TEST за выдающийся уровень защиты. Три из них получены за решения для частных устройств на Windows и Mac, а шесть — за продукты для корпоративной защиты.
- «Лаборатория Касперского» вновь успешно прошла независимый аудит Service and Organization Controls 2 второго типа (SOC 2 Type 2). Он подтверждает, что процессы разработки и выпуска антивирусных баз Компании безопасны и надежно защищены от несанкционированного вмешательства.
- Приложение родительского контроля Kaspersky Safe Kids снова признано одним из самых эффективных решений для защиты детей в интернете. Продукт получил сертификаты AV-TEST и AV-Comparatives за эффективность в блокировке неподходящего контента.

2025

- За 2025 год продукты «Лаборатории Касперского» приняли участие в 100 независимых тестированиях и обзорах. В 90 случаях они заняли первое место, в 94 — вошли в тройку лучших. Вхождение Компании в топ-3 за год составило 94%.
- VDC Research включила «Лабораторию Касперского» в число ключевых игроков мирового рынка решений информационной безопасности для промышленности, особо отметив XDR-платформу Kaspersky Industrial CyberSecurity (KICS) и открытие новых Центров прозрачности.
- Решение Kaspersky EDR Expert первым в индустрии успешно прошло все испытания в исследовании AV-Comparatives EDR Detection Validation Certification test 2025, заслужив награду Certified EDR Detection 2025.
- Решение Kaspersky Premium по итогам тестов AV-Comparatives показало максимальный результат, суммарно получив 105 баллов из 105 возможных.
- «Лаборатория Касперского» победила в трех главных номинациях премии SE Labs Security Awards. Награды получили решения Компании для защиты частных пользователей, малого бизнеса и крупных компаний.
- Решение для защиты бизнеса Kaspersky Endpoint Security вновь показало абсолютную эффективность против попыток вмешательства в его работу в тесте Anti-Tampering Test 2025 от AV-Comparatives.
- Frost & Sullivan и QKS Group признали «Лабораторию Касперского» лидером на мировом рынке Threat Intelligence, отметив глобальное присутствие Компании, технологичность и инновационность, обширное продуктовое портфолио, а также высокое качество работы с клиентами.
- Kaspersky Secure Connection отмечен наградой за высокую скорость работы на ежегодной сертификации AV-TEST. Он получил сертификат «Одобрено» за стабильное соединение, высокоэффективную защиту конфиденциальности пользователя и низкое влияние на производительность системы.
- ISG отметила эффективность «Лаборатории Касперского» в плане расширенного обнаружения и реагирования. Компания получила награды Global Product Challenger и «Лидер рынка» в Бразилии за свою технологию XDR.

Ключевые результаты в 2025 году

GRI 201-1, СОКБ 61

+23%
увеличение продаж решений в России и странах СНГ

$836 млн
глобальная выручка в фиксированных курсах за 2025 год[1]

+21%
увеличение глобальных продаж решений крупному бизнесу[1]

+30%
увеличение продаж новых перспективных решений и технологий, защищающих компании от самых сложных киберугроз (non-endpoint) в России

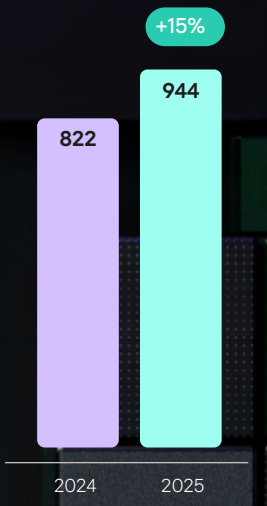
+24%
рост бизнеса в сегменте B2B в России и странах СНГ

+89%
рост продаж решений на базе KasperskyOS в России

+16%
рост бизнеса в сегменте B2B в мире

+16%
рост бизнеса в сегменте B2C в России и странах СНГ

Глобальная выручка в фактических курсах[2], $ млн



1 Консолидированные продажи (net sales) рассчитаны в долларах США с использованием фиксированных курсов валют 2025 года.
2 Результат глобального бизнеса «Лаборатории Касперского» в фактических курсах.

Управление устойчивым развитием

в 10 ЦУР ООН
вносит вклад Компания

в 5
национальных целей развития Российской Федерации вносит вклад Компания

Система управления устойчивым развитием

GRI 2-9, GRI 2-12, СОКБ 45

Вопросы, связанные с устойчивым развитием и воздействиями «Лаборатории Касперского», рассматриваются комплексно и на нескольких уровнях управления.

Совет директоров верхнеуровнево участвует в утверждении общих стратегических направлений и целей в области устойчивого развития. Контроль выполнения инициатив и мониторинг результатов осуществляются отделом проектов устойчивого развития совместно с руководителями проектных команд. Эти подразделения обеспечивают методологическую поддержку, анализ достигнутых результатов и регулярное обновление данных для внутренней отчетности.

Стратегические приоритеты в области устойчивого развития

«Лаборатория Касперского» придерживается пяти ключевых стратегических направлений в области устойчивого развития. Они определены исходя из специфики деятельности Компании, особенностей ее позитивных и негативных воздействий и влияют на разработку и реализацию ключевых ESG-инициатив

Ответственный подход к ведению бизнеса

- Развитие деловой этики и повышение устойчивости бизнеса
- Защита данных и соблюдение прав на приватность
- Обеспечение прозрачности кода и процессов

Вклад в развитие общества

- Социальные и благотворительные проекты
- Подготовка и развитие кадров для IT
- Сокращение цифрового неравенства, инклюзивность и доступность технологий
- Повышение цифровой грамотности в обществе

Уменьшение воздействия на окружающую среду

- Снижение углеродного следа и повышение энергоэффективности инфраструктуры
- Оптимизация потребления ресурсов
- Развитие экологической культуры и поддержка природоохранных инициатив

Глобальная киберустойчивость и безопасное цифровое будущее

- Защита пользователей, бизнеса и критической инфраструктуры от киберугроз
- Развитие кибериммунитета для новых перспективных технологий
- Международное сотрудничество в борьбе с киберпреступностью
- Формирование безопасной цифровой среды
- Внедрение инноваций, включая искусственный интеллект

Подход к управлению персоналом с акцентом на заботу о сотрудниках

- Создание благоприятной, инклюзивной и безопасной рабочей среды для сотрудников
- Развитие и поддержка персонала
- Поддержка женщин в IT

GRI 2-23, GRI 2-24

1. Антикоррупционная политика
2. Закупочная политика
3. Политика по контрактам
4. Политика в области охраны труда

Ключевые внутренние документы размещены во внутренних информационных системах и доступны для всех сотрудников «Лаборатории Касперского». Обязательства, закрепленные в этих документах, доводятся до сведения сотрудников в процессе оформления на работу и в ходе регулярного обучения внутри Компании.

Воздействия Компании в области устойчивого развития

Деятельность «Лаборатории Касперского» оказывает комплексное влияние на экономику, окружающую среду и общество. Компания стремится усиливать позитивные воздействия и снижать возможные негативные эффекты, связанные с операционной деятельностью и развитием цифровых технологий.

GRI 203-1, GRI 203-2

Экономика

+ Позитивные воздействия

- Улучшение цифровой безопасности бизнеса и организаций — защита от кибератак, снижение экономических потерь
- Создание решений для промышленной безопасности и критической инфраструктуры — поддержка более стабильной экономики

– Негативные воздействия

- Значительная доля рынка и высокий уровень технологической экспертизы Компании могут создавать барьеры для входа новых или нишевых игроков, что потенциально ограничивает конкуренцию на отдельных сегментах рынка кибербезопасности
- Повышение уровня цифровой безопасности требует от организаций дополнительных инвестиций в программную инфраструктуру и обучение персонала, что может увеличивать операционные издержки
- Внедрение сложных решений в области кибербезопасности может усиливать разрыв между организациями с высоким уровнем цифровой зрелости и теми, кто обладает ограниченными финансовыми и технологическими ресурсами

Окружающая среда

+ Позитивные воздействия

- Снижение доли физических упаковок и рост доли электронных лицензий — снижение объема потребления ресурсов
- Блокировка нелегального майнинга, что снижает потребление электроэнергии и, по оценкам Компании, обеспечивает сокращение до 3 тысяч тонн выбросов CO_2-экв. ежегодно.
- Оптимизация потребления ресурсов в офисах и дата-центрах

– Негативные воздействия

- Высокий углеродный след от авиаперелетов сотрудников, связанных с международными проектами, партнерскими встречами и мероприятиями
- Высокая энергоемкость дата-центров и серверов

Подробнее о снижении негативных воздействий читайте в разделах «Снижаем углеродный след» и «Энергоэффективность дата-центров» на с. 91 и 93

Люди

+ Позитивные воздействия

- Создание новых рабочих мест
- Социальный пакет для сотрудников
- Поддержка родительства
- Программы по цифровой грамотности, инклюзии, поддержка сотрудников с инвалидностью, участие в образовательных проектах

– Негативные воздействия

- Цифровое неравенство: часть населения не успевает за развитием технологий, что делает людей без цифровых навыков более уязвимыми
- Усложнение цифровой жизни: требования кибербезопасности делают повседневные действия сложнее, что особенно тяжело для пожилых людей и людей с когнитивными особенностями

Подробнее о снижении негативных воздействий читайте в разделе «Инклюзивность в киберпространстве» и «Цифровое просвещение» на с. 80 и 87

Вклад в решение общих задач

«Лаборатория Касперского» стремится вносить вклад в достижение глобальных и национальных приоритетов в области устойчивого развития. Компания поддерживает достижение Целей устойчивого развития (ЦУР) ООН и национальных целей развития Российской Федерации и фокусируется на тех из них, в рамках которых ее собственное влияние является наибольшим.

Вклад в достижение национальных целей развития Российской Федерации

Сохранение населения, укрепление здоровья и повышение благополучия людей, поддержка семьи

Вклад Компании связан с обеспечением достойных условий оплаты труда для сотрудников.

Подробнее читайте в разделе «Наша система мотивации» на с. 60

Технологическое лидерство

«Лаборатория Касперского» развивает отечественные инновационные технологии, в том числе искусственный интеллект.

Подробнее об инициативах читайте в разделе «Цифровая безопасность» на с. 49

Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы

Компания создает решения, которые способствуют цифровой трансформации и продвижению информационных технологий на уровне от государств и крупного бизнеса до частных пользователей.

Подробнее читайте в разделе «Цифровая безопасность» на с. 23

Устойчивая и динамичная экономика

Деятельность Компании прямо и косвенно способствует экономическому росту России.

Подробнее читайте в разделе «Цифровая безопасность» на с. 31

Реализация потенциала каждого человека, развитие его талантов, воспитание патриотичной и социально ответственной личности

«Лаборатория Касперского» создает и поддерживает образовательные проекты для сотрудников и местных сообществ, стажировки и реализует совместные проекты с НКО.

Подробнее читайте в разделах «Развитие сотрудников» и «Подготовка кадров для IT-отрасли» и «Цифровое просвещение» на с. 68, 82 и 87

Вклад в достижение ЦУР ООН

Образовательные проекты в «Лаборатории Касперского» создаются как для сотрудников, так и для местных сообществ.

Подробнее о проектах в сфере образования читайте в разделах «Развитие сотрудников» и «Подготовка кадров для IT-отрасли» и «Цифровое просвещение» на с. 68, 82 и 87

«Лаборатория Касперского» идет в авангарде продвижения женщин в IT-индустрии в России.

Подробнее о программах в области гендерного равенства читайте в разделе «Женщины в IT» на с. 63

В Компании действуют инициативы по снижению потребления энергии в офисах и ЦОД.

Подробная информация размещена в разделе «Повышаем энергоэффективность» на с. 92

Сотрудники — наш главный актив, и их удовлетворенность работой особенно важна для Компании.

Подробнее о создании достойных условий труда читайте в разделе «Люди в «Лаборатории Касперского» на с. 56

«Лаборатория Касперского» разрабатывает и внедряет уникальные инновационные решения в области кибербезопасности.

Подробнее об инновационных проектах читайте в разделе «Цифровая безопасность» на с. 49

Проекты Компании способствуют безопасному и устойчивому развитию городов и экономики в целом.

Подробнее о защите инфраструктуры городов читайте в разделе «Как мы защищаем критическую инфраструктуру» на с. 31

Компания стремится сокращать воздействие на окружающую среду и потребление ресурсов по всей цепочке поставок.

Подробнее об инициативах в области ответственного производства и потребления читайте в разделе «Окружающая среда» на с. 89

«Лаборатория Касперского» поддерживает проекты фонда «Природа и люди», включая программы по сохранению каланов и мониторингу состояния морских экосистем.

Подробнее об инициативах читайте в разделе «Развиваем экологическую культуру» на с. 98

Компания поддерживает мероприятия по сохранению популяций медновского песца и других видов, а также природоохранные экспедиции и проекты партнерских некоммерческих организаций (НКО) по сокращению числа бездомных животных.

Подробнее об инициативах читайте в разделе «Развиваем экологическую культуру» на с. 99

Взаимодействие с заинтересованными сторонами

GRI 2-29

«Лаборатория Касперского» придерживается подхода, основанного на уважении, открытом диалоге и ответственности, стремясь поддерживать устойчивые и доверительные отношения со всеми заинтересованными сторонами.

Сотрудники

Интересы группы

- Стабильное трудоустройство и карьерный рост
- Справедливая заработная плата и социальное обеспечение
- Комфортные и безопасные условия труда
- Обучение и развитие
- Отсутствие дискриминации

Способы взаимодействия

- Система внутрикорпоративных коммуникаций
- Встречи с руководителями Компании
- Совместные конференции, культурные и спортивные мероприятия
- Корпоративный сайт

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с сотрудниками читайте в разделе «Люди в «Лаборатории Касперского» на с. 56

Пользователи

Интересы группы

- Защита персональных данных
- Высокое качество продукции
- Высокий уровень сервиса
- Приемлемые цены на продукцию

Способы взаимодействия

- Система обратной связи и сервисы
- Пресс-релизы, рекламные и промоматериалы

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с пользователями читайте в разделе «Защита доверия пользователей» на с. 108

Партнеры и поставщики

Интересы группы

- Прозрачность и открытость конкурентных процедур
- Контроль за качеством продукции
- Соблюдение деловой этики
- Противодействие коррупции
- Своевременное и точное исполнение договорных обязательств

Способы взаимодействия

- Проведение открытых конкурентных процедур
- Оперативное рассмотрение претензий
- Деловые встречи, конференции и выставки
- Раскрытие информации

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с партнерами читайте в разделе «Устойчивая цепочка поставок» на с. 117

Органы государственной власти и правоохранительные органы

Интересы группы

- Соблюдение требований законодательства и стандартов
- Своевременная уплата всех применимых налогов и сборов
- Инвестиции в развитие регионов присутствия
- Содействие в обеспечении занятости и поддержка предпринимательства
- Обеспечение безопасности объектов критической инфраструктуры (КИ)
- Содействие борьбе с киберпреступлениями

Способы взаимодействия

- Консультации с сотрудниками правоохранительных органов
- Разработка программного обеспечения и предоставление лицензий
- Консультации по вопросам законотворчества

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с государственными и правоохранительными органами читайте в разделе «Как мы боремся с киберпреступностью» на с. 26

Местные сообщества

Интересы группы

- Создание рабочих мест для местных жителей, развитие человеческого капитала
- Вклад в развитие социальной инфраструктуры
- Развитие местных производств и поставщиков
- Благотворительные проекты и социальные инвестиции
- Минимизация негативного воздействия на окружающую среду территорий присутствия
- Информационная открытость и прозрачность деятельности

Способы взаимодействия

- Наем персонала из представителей местных сообществ
- Стажировки для студентов
- Программы развития и повышения квалификации для персонала
- Обучающие программы для широкого круга пользователей
- Закупки у местных поставщиков

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с местными сообществами читайте в разделе «Вклад в развитие общества» на с. 73

Уязвимые с точки зрения информационной безопасности группы

Интересы группы

- Обеспечение безопасности в интернете

Способы взаимодействия

- Проведение обучающих мероприятий для повышения цифровой грамотности

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с уязвимыми группами читайте в разделе «Цифровое просвещение» на с. 87

НКО

Интересы группы

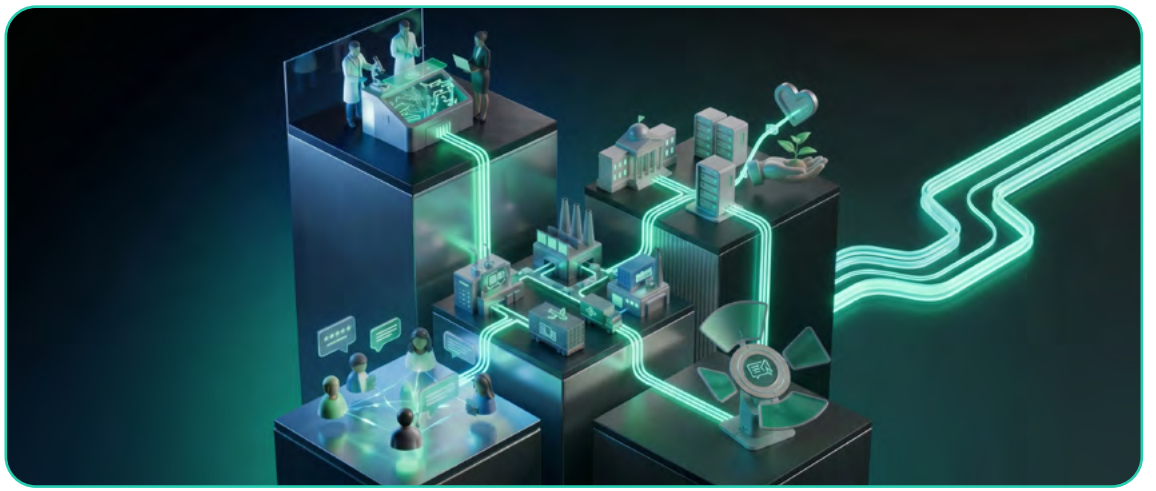
- Содействие в организации и реализации экологических и социальных программ

Способы взаимодействия

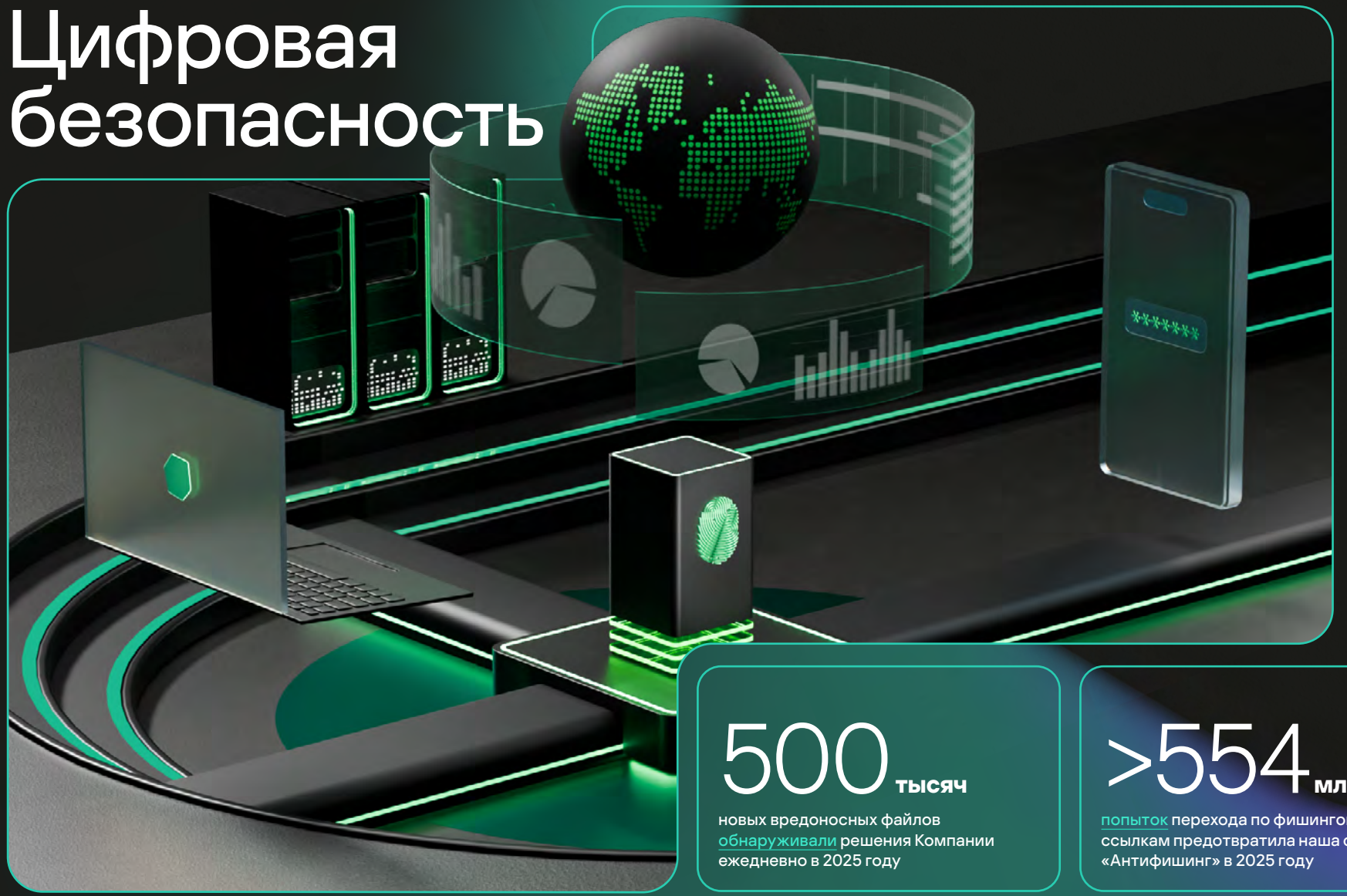
- Разработка, поддержка и проведение совместных экологических и социальных проектов

Результаты взаимодействия в отчетном периоде

Подробнее о взаимодействии Компании с НКО читайте в разделе «Социальные и благотворительные проекты» на с. 75



Цифровая безопасность



500 тысяч
новых вредоносных файлов обнаруживали решения Компании ежедневно в 2025 году

>554 млн
попыток перехода по фишинговым ссылкам предотвратила наша система «Антифишинг» в 2025 году

>3,5 млн
школьников прошли интерактивные тренажеры Компании в рамках проекта «Урок цифры» в 2025 году

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-угрозы[1] 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»

Сегодня экспертиза Компании сосредоточена в пяти профильных центрах, каждый из которых решает свои задачи, но при этом работает в тесной связке со всеми остальными. Вместе они позволяют не просто реагировать на угрозы, а понимать их природу, предугадывать развитие атак и превращать знания в надежную защиту.

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 Intelligence[1], 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.

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 помогали 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 стилерами[1] 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 (AFJOC[3]) во взаимодействии с правоохранительными 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 правоохранительные органы из 18 африканских стран и Великобритании для борьбы с программами-шифровальщиками, 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 мошенническую схему с инвестициями в криптовалюту, 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 злоумышленников превысил €3,5 млн.

Операция Serengeti

Сентябрь — октябрь 2024 года

Борьба с программами-шифровальщиками, BEC-атаками[2] 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 активности 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 необходимости 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 злоумышленники 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 сталкерского 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 продвинутых угроз

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 годом[1].

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 сталкерскому ПО.

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 — октябрем 2023 года.

Делимся экспертизой

Мы охотно делимся экспертизой в сфере кибербезопасности, выступая на крупных мероприятиях и организуя собственные конференции, такие как Security Analyst Summit, с участием представителей правоохранительных 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 кибербезопасности, в число которых вошли:

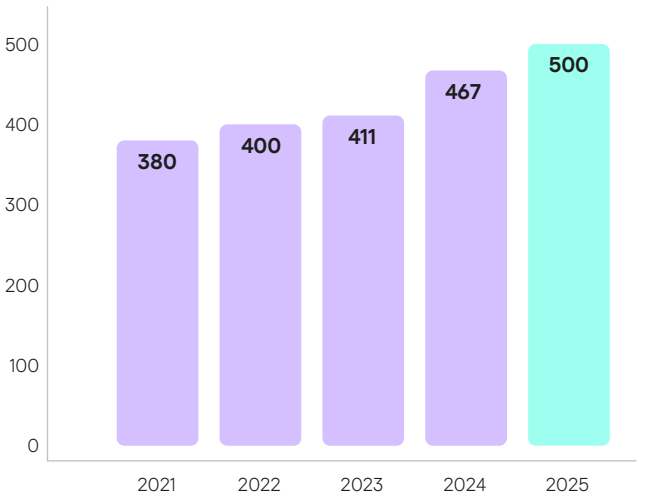
- рабочая группа открытого состава ООН по ИКТ (в рамках неформального диалога под эгидой председателя рабочей группы);
- консультации Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях;
- Форум ООН по управлению интернетом;
- Глобальный 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 правоохранительных 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 году[1].

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 началась в декабре 2024 года и была активна на протяжении многих месяцев. Атаки проводились преимущественно с часа ночи до пяти часов утра по местному времени — в это время злоумышленники пытались получить удаленный доступ к компьютеру 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 собственное вредоносное ПО, разработанное с применением искусственного интеллекта.
- Группа Angry Likho проводит атаки с января 2025 года, нацеливаясь на сотрудников корпораций России и Беларуси. В арсенале — стилеры для кражи конфиденциальных данных и утилиты удаленного администрирования для полного контроля над зараженным устройством.
- В 2025 году эксперты Kaspersky GReAT раскрыли схему, в которой злоумышленники украли у российского разработчика криптовалюту на сумму около $500 000 через зараженный пакет с открытым исходным кодом. Он мимикрировал под расширение 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

Как мы защищаем критическую инфраструктуру

Наша цель — обеспечить бесперебойное функционирование киберфизических систем на объектах критической инфраструктуры и в промышленности с помощью современных технологий, знаний и опыта.

Защищены решениями «Лаборатории Касперского»

>130
завершенных проектов в нефтегазовом секторе

>40
компаний энергетической и коммунальной отраслей

12%
мировой добычи нефти

>80
завершенных проектов в электроэнергетике (атомная, тепловая, ВИЭ)

Топ-5
глобальных производителей ВИЭ

>60
нефтегазовых компаний

Критическая инфраструктура (КИ) — это технологические системы, от которых напрямую зависит устойчивое функционирование экономики, государства и общества.

Примеры КИ

- Энергетика
- Водоснабжение
- Транспорт
- Добыча полезных ископаемых
- Металлургия
- Машиностроение
- Пищевая промышленность
- Химическая промышленность
- Фармацевтическая промышленность
- ЖКХ
- Логистика
- Производство электроники и др.

Почему это важно

Современные системы промышленной автоматизации становятся все более цифровыми, связанными и умными — они используют облака, ИИ, интернет вещей и цифровые двойники. Это повышает эффективность производства, но и увеличивает риски: возрастает поверхность атаки, а сами объекты КИ превращаются в привлекательную цель для злоумышленников. При этом многие критически важные системы изначально создавались для работы в изолированной среде, а сейчас вынуждены функционировать в условиях высокой открытости и связанности.

Сегодня мир сталкивается с растущим числом кибератак на критически важные объекты, и эти атаки становятся все более изощренными.

Ключевые инциденты 2024–2025 годов

- Служба военной разведки Дании 18 декабря 2025 года опубликовала заявление, в котором утверждалось, что группа Z-Pentest провела разрушительную атаку на Датский водоканал в 2024 году. Атакующие изменили давление в насосной станции недалеко от города Кёге, что привело к прорыву трех труб.
- Атака вымогателей на Jaguar Land Rover вызвала пятинедельный простой производства, ставший прямой причиной убытков, оцениваемых в десятки миллионов долларов. Инцидент стал фатальным для нескольких поставщиков автопроизводителя — им пришлось прибегнуть к процедуре банкротства. Атака сказалась на работе около 5 000 британских организаций, нанеся суммарный ущерб британской экономике в $2,5 млрд.
- Атака вымогателей на платформу онлайн-регистрации ARINC cMUSE американского разработчика Collins Aerospace привела к сбоям в работе нескольких крупнейших европейских аэропортов, в очередной раз демонстрируя, насколько авиатранспортный сектор уязвим к атакам на цепочку поставок.
- Крупнейшая российская авиакомпания «Аэрофлот» также стала жертвой злоумышленников. Атака хактивистов на системы авиакомпании вынудила отменить множество рейсов.
- Неизвестные злоумышленники в апреле 2025 года атаковали плотину на озере Рисеватнет в коммуне Бремангер на западе Норвегии и дистанционно открыли затвор. Он был полностью открыт в течение четырех часов, прежде чем несанкционированное вмешательство обнаружили и локализовали.

Все чаще уязвимыми оказываются энергетика, водоснабжение и транспорт — отрасли, от которых напрямую зависят повседневная жизнь людей и устойчивое развитие страны.

В то же время основной мишенью злоумышленников остается именно производственный сектор. Согласно нашим ежеквартальным обзорам основных инцидентов промышленной кибербезопасности, подавляющее большинство атакованных в 2024–2025 годах организаций относятся к производству.

Наш подход к защите критической инфраструктуры

Мы рассматриваем кибербезопасность как непрерывный цикл: подготовка — мониторинг и своевременное обнаружение — реагирование — быстрое восстановление работы.

Сегодня киберустойчивость выходит за рамки классической кибербезопасности. Это означает, что уже недостаточно просто блокировать атаки — нужно обеспечивать устойчивость всей OT-инфраструктуры[1] даже в условиях инцидентов.

Поэтому мы строим платформу безопасности киберфизических систем, где решения «Лаборатории Касперского» защищают ИТ-, OT- и IIoT-среды[2], помогают организациям внедрять цифровые технологии, не ставя под угрозу стабильность бизнеса, безопасность людей и окружающей среды.

Помогаем минимизировать риски и оценивать выгоды от инвестиций в защиту КИ

Как наши решения помогают бизнесу экономить и принимать взвешенные решения

Нарушения в работе промышленных предприятий из-за кибератак могут обернуться серьезными убытками — от простоя оборудования до потери продукции и репутационного ущерба. Чтобы помочь компаниям точнее оценивать риски и эффективность инвестиций в кибербезопасность, мы провели международное исследование совместно с аналитическим агентством VDC Research.

Что в результате

Совместное исследование показало, что внедрение комплексного решения (защита промышленных узлов и мониторинг сетевого трафика) может снизить потенциальный ущерб от киберинцидентов:

- **до 45%** — для предприятий энергетики и ЖКХ;
- **до 76%** — для производственного сектора.

[1] OT-инфраструктура (Operational Technology) — совокупность систем, оборудования и ПО, которые напрямую управляют физическими процессами в промышленности и на объектах критической инфраструктуры.

[2] Industrial Internet of Things или промышленный интернет вещей — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

Обеспечиваем защиту на всех уровнях

Платформа промышленной безопасности KOTCS

Kaspersky OT CyberSecurity — это специализированная XDR-платформа, которая защищает все уровни систем и сетей промышленных предприятий и объектов критической инфраструктуры.

Уровень 2

Мониторинг и управление

- IIoT[1], защита периметра и верхнего уровня автоматизации (SCADA)
- Контроль доступа, аудит и повышение видимости OT-систем
- Экспертная поддержка на стороне заказчика

Уровень 3

Корпоративные системы

- Конвергенция IT и OT, корреляция данных из всех доступных источников
- Унифицированные процессы и подходы к обеспечению безопасности с помощью технологии расширенного обнаружения и реагирования на угрозы гибридного типа (Hybrid XDR)
- Обучающие программы, консалтинг и расширенная аналитика угроз

Уровень 1

Контроллеры и защита

- Обнаружение вторжений, попыток взлома и компрометации микропроцессорного оборудования нижнего уровня автоматизации
- Глубокая инспекция промышленных протоколов (DPI), защита встроенных ОС от сетевых угроз и попыток изменения параметров технологического процесса
- Обнаружение аномалий в техпроцессах с помощью машинного обучения

Уровень 0

Технологический процесс

- Мониторинг киберфизических угроз для основного оборудования
- Обеспечение безопасности подключенных транспортных средств и других физических объектов

[1] Industrial Internet of Things или Промышленный интернет вещей — многоуровневая система, включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты.

Ключевые отрасли применения

- Нефтегазовая и химическая отрасли
- Электроэнергетика, включая атомную, и ЖКХ
- Металлургия и добыча полезных ископаемых
- Промышленное производство, в том числе микроэлектроника

Перспективные направления применения Kaspersky OT CyberSecurity

- Фармацевтика и медтехника
- Транспорт и логистика, включая аэропорт
- Телекоммуникации
- Крупные объекты инфраструктуры (стадионы, бизнес-центры, торговые центры, жилые комплексы)

Специализированные решения

- Kaspersky SD-WAN
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky Antidrone

Kaspersky Industrial CyberSecurity

Нативный XDR

KICS for Nodes

Защита конечных точек, обнаружение и реагирование

KICS for Networks

Анализ сетевого трафика, обнаружение и реагирование

Решения на базе KasperskyOS

- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Знания

Кибергигиена	Аналитика угроз	Обучение
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Экспертиза

Диагностика	Реагирование	Управляемый сервис
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

KICS — основа платформы Kaspersky OT CyberSecurity

Сегодня под защитой KICS

12%
общемировой добычи нефти и газа

10%
нефтехимического производства

до 15–25%
добычи и переработки различных металлов

15%
коммерческой атомной генерации

20%
производства азотных и фосфорных удобрений

Ядром платформы киберфизической безопасности является Kaspersky Industrial CyberSecurity (KICS). Решение обеспечивает ситуационную осведомленность, киберустойчивость, видимость событий в промышленных сетях и мощную защиту основных автоматизированных систем, не влияя на доступность технологических процессов.

KICS помогает предотвратить дорогостоящие простои, инциденты безопасности, кражу данных и саботаж, вызванные массовыми угрозами, целевыми атаками, программами-вымогателями или действиями инсайдеров. Она также позволяет защитить устаревшее оборудование и продлить срок его эксплуатации, помогает соблюдать национальные и международные стандарты и лучшие практики информационной безопасности промышленных инфраструктур.

Состав платформы:
- KICS for Nodes — защита серверов, рабочих станций, панелей оператора на базе Linux и Windows;
- KICS for Networks — анализ сетевого трафика, инвентаризация активов, выявление аномалий и вторжений, реагирование на сетевые угрозы.

География распространения KICS

За отчетный период мы существенно укрепили отношения с компаниями, которые специализируются на системах хранения энергии, производстве электротранспорта и солнечных панелей. Среди наших клиентов пять производственных компаний, каждая из которых, по независимым оценкам, входит в топ-5 мировых лидеров в этих отраслях.

Такое взаимодействие придало бизнесу дополнительный импульс, результатом которого стала организация в 2025 году конференции KICS Con China 2025 в Шэньчжэне — одном из инновационных регионов, известном своим технологическим кластером. Эта конференция собрала более 100 участников. Также были проведены отраслевые круглые столы для нефтегазового сектора в регионе META[1].

Мы последовательно развиваем программу технологического партнерства. Платформа KICS прошла испытания на совместимость с решениями производителей промышленной автоматизации из Латинской Америки, Восточной Азии и Китая, включая Altus, Chint, Consen, Supcon и HollySys, помогая заказчикам выстраивать устойчивые цепочки поставок и ответственно подходить к выбору технологий.

В настоящее время KICS — лидер по числу публичных историй успеха как в портфолио «Лаборатории Касперского», так и среди конкурентов.

Наши новые клиенты, защищенные KICS:
- Nuevo Hospital de Toledo (Испания) — самый большой госпиталь в регионе Иберия;
- Birla Sugar Group — крупнейший в Индии производитель сахара;
- Holy Stone — один из лидеров цементной отрасли в Китае;
- Atlas Tapes (Греция) — крупнейший в Евросоюзе производитель изоленты;
- OLED — крупнейший в Китае производитель OLED-дисплеев.

Платформа KICS совместима со множеством АСУ ТП от
70+ вендоров

>50
успешных историй внедрения KICS

[1] Ближний Восток, Турция, Африка.

Платформа XDR для промышленности

Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика, обнаружение и реагирование

Kaspersky Industrial CyberSecurity for Nodes

Защита конечных точек, обнаружение и реагирование

- Обнаружение активов
- Уязвимости и риски
- Видимость сети
- Набор инструментов анализа трафика

- Обнаружение вторжений
- Обнаружение аномалий
- Глубокий анализ промышленных протоколов (DPI)
- Корреляция событий
- Умное присвоение приоритетов инцидентам

Набор интеграций со сторонними решениями и синергия внутри экосистемы Kaspersky OT Cybersecurity

- Расширенный мониторинг хостов
- Инвентаризация оборудования и приложений
- Покрытие «слепых зон» (режим без SPAN-порта)

- Инциденты на стыке хоста и сети
- Граф расследования
- Обогащение оповещений
- Ручные действия по реагированию
- Ограничение сетевого доступа

- Сканирование уязвимостей
- Аудит соответствия
- Мониторинг изменений конфигурации

- Предотвращение угроз в реальном времени
- Контроль локальной активности
- Контроль сетевой активности
- Мониторинг системы

- Телеметрия с конечных точек (процессы, файлы и сетевая активность)
- Цепочка разработки (эволюции) угроз
- Меры реагирования

- Сканер вредоносного ПО
- Уязвимости
- Соответствие требованиям
- Захват трафика
- Инвентаризация узлов

Формируем кибериммунитет

Почему это важно

Кибериммунитет — свойство системы, при котором стоимость атаки на нее превышает потенциальный ущерб или выгоду злоумышленников. Мы считаем, что подобные системы можно создавать с помощью KasperskyOS. Для этого в KasperskyOS комбинируются лучшие практики разработки информационных систем с опорой на безопасную архитектуру, принципы и паттерны проектирования безопасных систем, контроль качества, методологию разработки безопасного ПО, отраслевые стандарты и обязательное тестирование на проникновение. Так мы приближаем прекрасное будущее, в котором системы решают задачи безопасности «из коробки».

Мы предлагаем строить системы так, чтобы они были безопасны по умолчанию благодаря разделению на изолированные части и контролю взаимодействий между ними.

В результате, даже если злоумышленнику удастся преодолеть одну линию защиты, остальные части системы продолжают работать безопасно. Это особенно важно для промышленной автоматизации, носимых устройств, интернета вещей и удаленного доступа к критической инфраструктуре.

Новые стратегические альянсы

- Соглашение с ОАО «РЖД» о тестировании и внедрении решений на базе KasperskyOS и технологий защиты контейнерных сред
- Соглашение с Институтом системного программирования РАН о создании Центра конструктивной информационной безопасности

KasperskyOS

Платформой для построения кибериммунных решений является микроядерная KasperskyOS. Это собственная разработка «Лаборатории Касперского», которая не основывается на каком-либо существующем открытом проекте.

Комбинация микроядерной архитектуры и концепций MILS (Multiple Independent Levels of Security) и FLASK (Flux Advanced Security Kernel) в KasperskyOS формирует принципиально новый уровень киберзащиты, позволяющий значительно повысить устойчивость системы к кибератакам.

В 2024–2025 годах мы сделали значительный шаг в развитии KasperskyOS: скорректировали стратегический фокус и начали расширять границы ее применения в качестве полноценной операционной системы общего назначения.

Флагманский релиз: Kaspersky Thin Client 2.3

Ключевым продуктом отчетного периода стала новая коммерческая версия Kaspersky Thin Client 2.3, которая объединила разработки 2024 и новые функции 2025 года:

- расширенную поддержку периферии (веб-камер, гарнитур, сканеров);
- централизованное управление настройками мониторов через Kaspersky Security Center;
- техподдержку удаленного администратора;
- режим Secure Boot.

Это первый релиз, сертифицированный на платформе Dell Wyse 3040, что стало важным шагом к расширению аппаратной совместимости.

Примеры успешного внедрения Kaspersky Thin Client

- Российская компания «КрасЭко» построила на базе этого решения безопасную инфраструктуру рабочих мест с единой консолью управления и поддержкой отечественных операционных систем.
- Международный партнер Aswant Distribution стал эксклюзивным дистрибьютором Kaspersky Thin Client в Малайзии и Индонезии. За 2024–2025 годы он поставил кибериммунные тонкие клиенты госорганам, промышленным предприятиям, финансовым и образовательным учреждениям региона.
- В муниципальном совете Кулима внедрение системы снизило операционные затраты на 20% и повысило киберустойчивость инфраструктуры.

Создаем продукты, позволяющие отслеживать ESG-показатели

Kaspersky Automotive Secure Gateway

Kaspersky Automotive Secure Gateway — это решение для защиты подключенных транспортных средств, включающее шлюз безопасности, бортовую систему обнаружения и предотвращения вторжений (In-Vehicle IDPS), сервисы телеметрии, дистанционного управления и навигационную систему.

Забота об экологии

Наше решение может осуществлять постоянный мониторинг систем автомобиля (батарея, электроника, параметры движения и прочее), что позволяет, например, оптимизировать зарядные операции и продлить срок службы аккумуляторов, а также сократить пробег сервисных машин и, соответственно — выбросы CO_2, используя данные предиктивной диагностики.

Безопасность людей

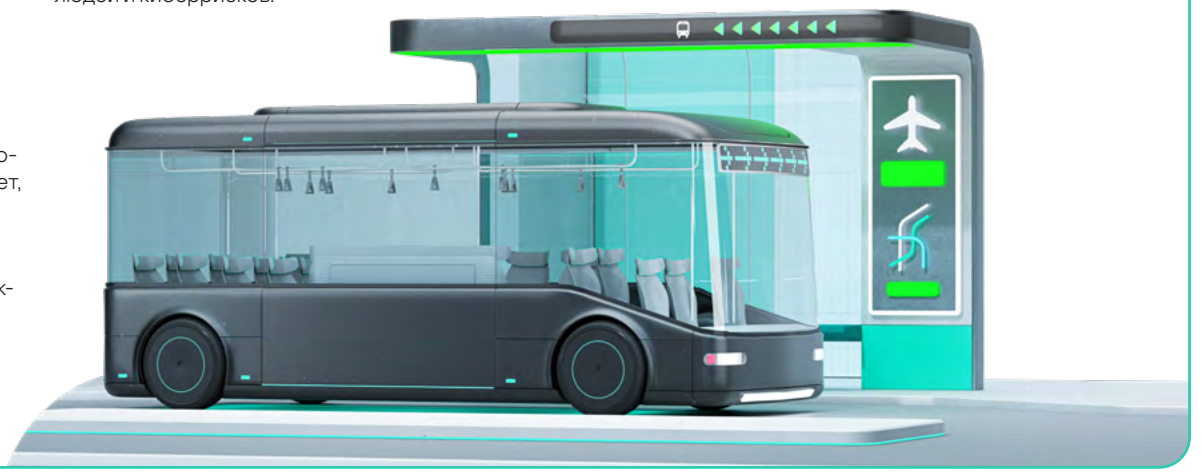
Наше решение — первое в России, процессы разработки которого и отдельные программные компоненты сертифицированы по ISO 26262 (ASIL B). Этот стандарт функциональной безопасности для автопрома минимизирует риски ущерба жизни и здоровью людей в результате сбоев автомобильных систем.

Учет требований информационной (security) и функциональной (safety) безопасности открывает путь к удаленным бизнес-сценариям (дистанционное обслуживание, автономные перевозки, гибкие рабочие модели доступа к транспортным средствам) без компромиссов в области безопасности людей и киберрисков.

Качество управления

Kaspersky Automotive Secure Gateway помогает автопроизводителям соблюдать требования международных стандартов кибербезопасности для транспортных средств, в том числе обеспечивая мониторинг событий ИБ и их передачу в Vehicle Security Operations Center (VSOC) для своевременного реагирования и расследования инцидентов.

Такие свойства Kaspersky Automotive Secure Gateway способствуют реализации ESG-принципов в транспортной отрасли.



Соблюдаем требования и стандарты при разработке решений

«Лаборатория Касперского» гарантирует соответствие своих продуктов стандартам и законодательным требованиям к промышленной кибербезопасности в разных странах.

Подробнее о законодательных и отраслевых требованиях, которые мы учитываем при разработке наших продуктов и решений, читайте в приложении 5 на с. 136

KICS — первая в мире XDR-платформа, сертифицированная по промышленному стандарту IEC 62443-4-1

Оба продукта, входящие в платформу KICS, — KICS for Nodes и KICS for Network, — прошли сертификацию по основным международным стандартам в области кибербезопасности, а также учитывают или помогают исполнить требования других международных законов и отраслевых стандартов.

Наши результаты

Kaspersky OT CyberSecurity в 2024–2025 годах

Платформа промышленной безопасности Kaspersky OT CyberSecurity и входящее в нее решение Kaspersky Industrial CyberSecurity в отчетном периоде показали уверенный рост продаж. Повышение интереса к этим решениям было обусловлено:

- рыночными факторами, включая рост числа атак на промышленные предприятия, усиление региональных регуляторных норм, импортозамещение, фокус на киберсуверенитет и диверсификацию поставщиков средств защиты, рост зрелости заказчиков;
- долгосрочной стратегией «Лаборатории Касперского» по закреплению позиций на домашних рынках и геоэкспансии;
- стратегическим подходом к кросс-продуктовым экосистемным продажам для заказчиков государственного сектора и объектов критической инфраструктуры.

2-е место
в портфеле Kaspersky по суммарным продажам всех продуктов экосистемы

+20%
CAGR (среднегодовой совокупный темп роста) год к году

16%
выручки Компании генерируют промышленные заказчики (второе место после госсектора)

KICS в 2025 году

Платформа KICS показала стабильный 30%-ный годовой рост бизнеса, продемонстрировав хорошую динамику на всех ключевых рынках, включая регионы, затронутые геополитическими проблемами.

- Российский рынок остается ключевым для KICS, генерируя 75% бизнеса и сохраняя снизившиеся по сравнению с предыдущими периодами, но все еще высокие темпы роста в 25%. Это обусловлено ужесточением законодательства в разрезе защиты КИИ, продолжающимися тенденциями импортозамещения и большим числом атак на инфраструктуру.
- Международные продажи растут более чем на 50% год к году благодаря реализуемой Компанией стратегии геоэкспансии.

KasperskyOS

В 2024–2025 годах экосистема KasperskyOS продемонстрировала устойчивый рост и выход на новые рынки. Портфель решений на ее базе расширился, охватив корпоративный, транспортный и встраиваемый сегменты. В этот период платформа показала двухзначный по миру и трехзначный в России рост инсталляционной базы (в процентном выражении).

+20%
рост продаж в России

Топ-5
доменов среди B2B-продуктов Компании

>540
защищенных сетей крупных структурообразующих для экономики заказчиков

+20%
рост ARPC (среднего дохода на одного клиента) за счет cross-sell и up-sell решений (кросс-продаж и увеличения объема продаж существующим клиентам)

>330 000
проданных лицензий

Наши планы на 2026–2027 годы

Промышленная кибербезопасность

Промышленные компании по всему миру переходят от закрытых (проприетарных) решений к открытым архитектурам и программно-определяемой автоматизации. Например, в России уже создана Межотраслевая рабочая группа по вопросу разработки открытой автоматизированной системы управления технологическими процессами (АСУ ТП).

В связи с этим наши планы в сфере промышленной кибербезопасности на 2026–2027 годы включают:

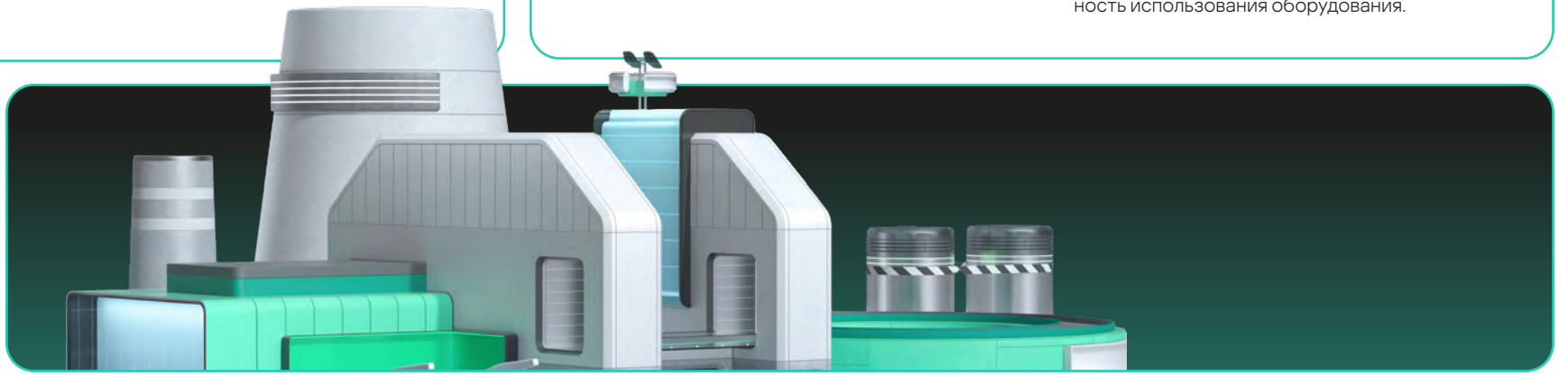
1. **Интеграцию и развитие KICS.** В рамках развития Kaspersky OT CyberSecurity мы планируем продолжать интеграцию KICS с решением для защиты облачных и контейнерных сред Kaspersky Cloud Workload Security, параллельно расширяя ее функциональность и интеграцию с другими продуктами. В KICS уже применяются технологии ИИ для мониторинга (профилирование устройств, анализ процессов) и разрабатываются средства защиты от будущих кибератак с использованием ИИ.
2. **Развитие кибериммунных устройств и новых технологий.** Еще одно направление развития KOTCS — разработка на базе KasperskyOS кибериммунных устройств — тонких клиентов и защищенных мобильных устройств. Также в планах — развитие от шлюзов подключенных автомобилей к устройствам контроля данных V2X[1] для высокоавтоматизированных транспортных средств. Они не требуют экстренных обновлений безопасности и служат дольше.
3. **Подготовку специалистов.** Совместно с Kaspersky Academy мы планируем развивать сотрудничество с ведущими техническими вузами, в которых есть кафедры или учебные лаборатории АСУ ТП или информационной безопасности. Предлагая студентам возможность получить актуальный практический опыт, мы уже сейчас формируем кадровый резерв инженеров, которые будут защищать критически важные предприятия в течение будущих десятилетий.

Развитие KasperskyOS

KasperskyOS в ближайшие годы сфокусируется на выходе за рамки ниши встроенных решений и превращении в полноценную технологическую основу для безопасных цифровых экосистем нового поколения.

Основные направления развития экосистемы

1. **Расширение областей применения.** KasperskyOS станет универсальной защищенной платформой для цифровых экосистем компаний, государственных структур и промышленных организаций.
2. **Технологическое развитие ядра и SDK.** Улучшение микроядерной архитектуры, оптимизация производительности и расширение инструментов для разработчиков (KasperskyOS SDK) — это позволит партнерам и разработчикам быстрее создавать новые решения на базе ОС.
3. **Рост экосистемы.** Формирование сообщества интеграторов и разработчиков, использующих KasperskyOS, расширение образовательных программ и акселераторов по кибериммунной безопасности.
4. **Международное продвижение.** Масштабирование внедрения KasperskyOS в странах Азии, Ближнего Востока, Латинской Америки и Турции, создание региональных центров компетенций и развитие локализованных версий продуктов.
5. **Регуляторное и отраслевое признание.** Продолжение совместной работы с регуляторами и промышленными ассоциациями над формированием стандартов нового класса — устройств и систем со встроенной кибериммунной защитой, подтвержденной архитектурно.
6. **Вклад в ESG-повестку.** Использование KasperskyOS как основы для построения безопасных и энергоэффективных решений в транспорте, промышленности, энергетике и IT, чтобы помочь снизить углеродный след и повысить эффективность использования оборудования.



[1] Vehicle-to-Everything — обмен информацией в реальном времени между подключенным транспортным средством и любым другим объектом (другие транспортные средства, объекты дорожной инфраструктуры: светофоры, пешеходы, сети и др.) посредством технологий беспроводной связи.

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».

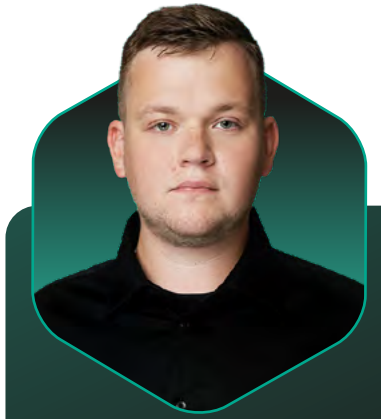
Реагируем на рост количества мобильных угроз

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 развивает 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 точечно 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 — простои, сбои 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 млн[1].

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 удостаивалась 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

На специальном сайте участники могли в игровой форме получить практические рекомендации по защите данных, соблюдению требований законодательства и снижению вероятности финансовых и репутационных потерь.

«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

Как мы защищаем разные группы пользователей

GRI 3-3

Защита разных групп пользователей — важная часть нашей работы по созданию более безопасного цифрового пространства.

Боремся с киберсталкингом

Что такое сталкерское ПО и чем оно опасно

Современные технологии стали важной частью жизни и во многом помогают нам, но иногда их используют во вред. Одна из таких угроз — цифровое преследование или кибersталкинг.

Злоумышленники могут установить на смартфон жертвы специальное приложение — так называемое сталкерское ПО (stalkerware). Такое ПО работает скрытно и тайно следит за человеком через его устройство: собирает информацию о местоположении, читает переписки, получает доступ к фотографиям и другим личным данным без ведома владельца смартфона. Это серьезная проблема, причем не только техническая, но и социальная, поскольку она нарушает право человека на приватность и часто может быть связана с домашним насилием.

Масштаб проблемы

23%

посетителей мировых сервисов онлайн-знакомств сталкивались с онлайн-преследованием

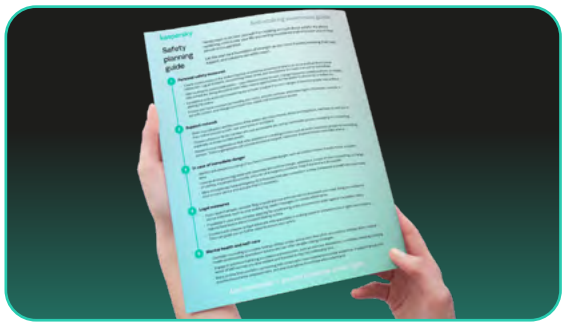
34 тысячи

пользователей во всем мире столкнулись со сталкерским ПО в 2024–2025 годах

Исследования «Лаборатории Касперского» показывают, что цифровое преследование — актуальная угроза.

Опрос, проведенный Компанией в России, выявил отношение респондентов к различным формам цифрового преследования со стороны бывших или нынешних партнеров, — вне зависимости от того, сталкивались респонденты с подобным или нет. Больше половины опрошенных боятся ситуаций с требованием предоставить доступ к личным данным на смартфоне, примерно столько же — слежки через сталкерские программы и трекеры (беспроводные метки). При этом последние два способа слежки сильнее беспокоят женщин, чем мужчин. Проблема цифровой слежки не ограничивается одной страной: по результатам глобального исследования «Лаборатории Касперского»[1], примерно каждый четвертый пользователь сервисов онлайн-знакомств (23%) сталкивался с той или иной формой цифрового преследования.

Обнаружить сталкерские приложения без специальных средств очень трудно. В случае обнаружения подозрительного приложения эксперты советуют не удалять его сразу (преследователь может быстро узнать об этом), а обратиться за помощью к специалистам, в кризисный центр или полицию.



Помогаем пользователям защищать себя

«Лаборатория Касперского» уже много лет защищает пользователей от цифрового преследования, возглавляя борьбу с кибersталкингом. В 2019 году мы внедрили в наше мобильное приложение функцию обнаружения сталкерских программ. Наше решение Kaspersky для Android сканирует устройство и предупреждает пользователя при выявлении скрытых приложений для слежки.

В 2024 году мы пошли дальше и добавили в приложение функцию «Кто за мной следит?», которая усиливает защиту сразу на нескольких уровнях. Она находит в телефоне незаметно установленные сталкерские приложения, обнаруживает поблизости подозрительные Bluetooth-метки и другие устройства слежения, а также показывает, какие разрешения выданы приложениям, нет ли среди них лишних, упрощающих слежку. Благодаря этому пользователь может вовремя заметить угрозу и сохранить контроль над своей безопасностью.

Помимо технических решений против сталкинга, Компания уделяет большое внимание просвещению и сотрудничеству.

В ноябре 2024 года мы опубликовали «Руководство по противодействию преследованию» — Anti-Stalking Awareness Guide, созданное совместно с международными экспертами и жертвами сталкинга. Цель инициативы — поддержать пострадавших и их близких, повысить осведомленность о проблеме и предоставить практические инструменты для защиты. Руководство помогает разобраться в природе сталкинга, опровергает распространенные мифы и описывает манипулятивные методы, которые используют преследователи. Центральное место в нем занимают два практических чек-листа, охватывающие как цифровую, так и физическую безопасность.

[1] В исследовании участвовали 21 000 человек по всему миру.

Первый чек-лист включает рекомендации по составлению плана безопасности, форму для документирования инцидентов, а также советы для родственников и друзей, поддерживающих пострадавших. Он был создан при участии:

- Олимпии Корал Мело Крус — активистки, инициировавшей «Закон Олимпии» в Латинской Америке, который стал основой для борьбы с цифровым насилием;
- Марселы Эрнандес — сооснователь Red Latinoamericana de Defensoras Digitales, сети поддержки защитников цифровых прав;
- Жанайны Кампос — бразильского психоаналитика, работающего с дисфункциональными отношениями;
- Акасии Дианы и Юлии Павловой — жертв сталкинга, которые поделились личными историями, чтобы повысить осведомленность других женщин.

Второй чек-лист — гид по цифровой безопасности (Digital Security Guide), разработанный экспертом «Лаборатории Касперского» Анной Ларкиной, — содержит рекомендации по защите личных данных, настройке приватности и снижению цифровых рисков, которые могут сделать человека уязвимым к онлайн-преследованию. Вместе эти материалы формируют целостный подход к поддержке пострадавших, охватывая как защиту физической безопасности, так и обеспечение цифровой защиты, и подчеркивают приверженность «Лаборатории Касперского» созданию более безопасного цифрового пространства для всех.

Кроме того, эксперты Компании регулярно делятся советами по цифровой безопасности. Например, мы рекомендуем использовать сложные уникальные пароли и не делиться ими, тщательно настраивать приватность в соцсетях и не раскрывать слишком много личной информации в интернете. Такие простые меры снижают риски и помогают чувствовать себя увереннее.

Объединяем усилия и помогаем жертвам

>40

организаций входят в международную Коалицию по борьбе со сталкерским ПО, сооснователем которой стала «Лаборатория Касперского»

Противодействие кибersталкингу требует объединения усилий многих участников, и Компания активно работает в этом направлении. В 2019 году мы стали сооснователем международной Коалиции по борьбе со сталкерским ПО (Coalition Against Stalkerware), которая сегодня объединяет более 40 организаций — от IT-компаний до правоохранительных органов. Вместе с партнерами мы повышаем осведомленность о цифровом насилии и помогаем пострадавшим.

«Лаборатория Касперского» участвует в международных инициативах по борьбе с цифровым насилием, например в европейском проекте DeStalk. Еще один совместный проект — исследование «Как защитить жертв насилия со стороны партнера от рисков, связанных с цифровыми технологиями»[1]. Кроме «Лаборатории Касперского», в нем участвуют другие международные компании, представители академического сообщества и некоммерческие организации. Проект реализуется в партнерстве с британским агентством UKRI с 2023 по 2026 год. Компания поддерживает его своей экспертизой в области противодействия кибернасилию и сталкингу, а также участием в дополнительных мероприятиях.

[1] How to protect victims/survivors of Intimate Partner Violence (IPV) from the risks created by digital technologies.

Безопасное пространство для тех, кому нужна защита

Поддерживаем Нижегородский женский кризисный центр

Мы понимаем, что за каждой цифрой статистики стоят реальные судьбы, поэтому стараемся участвовать в инициативах по помощи жертвам в реальной жизни.

Проблема
Женщины и дети, столкнувшиеся с домашним насилием и преследованием, часто нуждаются в срочном и безопасном убежище. При этом иногда у пострадавших нет доступа даже к собственным документам и деньгам. В такой ситуации во многих регионах у них нет шансов найти экстренное убежище.

Что сделано
С 2022 года «Лаборатория Касперского» поддерживает проект «Безопасная квартира» Нижегородского женского кризисного центра. Это секретное жилье, куда пострадавшие могут заселиться прямо в день обращения. Подопечным предоставляются базовые вещи: проживание, питание, одежда, связь, а также психологическая, юридическая и социальная помощь. Проект работает без формальных барьеров даже при отсутствии документов.

Результат
За четыре года фонду удалось помочь 32 женщинам с детьми.

Обеспечиваем онлайн-безопасность детей

Создание безопасной онлайн-среды для детей — задача первостепенной важности, от которой зависит наше будущее. «Лаборатория Касперского» работает над этим как своими силами, так и в партнерстве с министерствами, ведомствами и другими организациями по всему миру.

Почему это важно

Дети сегодня начинают пользоваться интернетом с самого раннего возраста — для учебы, общения и развлечений. Онлайн-среда дает много возможностей для развития, но вместе с тем несет и реальные риски: угрозы мошенничества, кибербуллинга, опасного контента, попытки манипуляции и давления. Часто дети сталкиваются с такими угрозами раньше, чем успевают понять, как им противостоять, а взрослые не всегда знают, что именно происходит с ребенком в цифровом пространстве.

Мы убеждены: чтобы защитить детей в интернете, недостаточно только технологий. Важно понимать, как именно они живут онлайн, чему доверяют, чего боятся и с какими проблемами сталкиваются. Поэтому «Лаборатория Касперского» много лет подряд проводит опросы на тему цифровых привычек детей и родителей, а затем превращает полученные знания в практические решения — образовательные программы, полезные материалы и инициативы, доступные семьям, школам и сообществам в разных странах.

О чем говорят наши исследования?

Один из ключевых проектов Компании в области обеспечения цифровой безопасности детей — регулярное исследование, на основе которого мы готовим аналитический отчет «Взрослые и дети в интернете». В 2024 году в нем участвовали 2 026 респондентов из крупных городов России — 1 013 пар «родитель — ребенок» (дети от 3 до 17 лет). Опрос охватывал повседневную цифровую жизнь: использование соцсетей и онлайн-сервисов, игры, общение, а также столкновения с мошенничеством, кибербуллингом и небезопасным контентом.

Мы также изучаем, как злоумышленники используют популярность детских брендов. Так, в отчетном периоде наши эксперты проанализировали угрозы, использующие в качестве приманки упоминание известных игр, игрушек и мультфильмов (Minecraft, Roblox, LEGO, Disney и др.). Исследование показало, что только за первый квартал 2024 года число таких атак выросло на 35% по сравнению с годом ранее.

В 2025 году мы продолжили анализировать цифровые привычки детей, используя обезличенные данные решения Kaspersky Safe Kids. Они показывают, что дети все больше времени проводят в онлайн-играх, видеоплатформах и социальных сервисах, чаще используют мобильные устройства и активно интересуются игровым и видеоконтентом.

При этом для них сохраняются ключевые риски — столкновения с мошенничеством, нежелательным контентом и попытками давления со стороны незнакомых пользователей. Эти данные подтверждают необходимость комплексного подхода к детской онлайн-безопасности, сочетающего технологическую защиту, обучение и развитие цифровой грамотности детей и родителей.

Результаты исследований

Основные тренды цифрового поведения детей в 2024–2025 годах

- 54% детей 3–6 лет регулярно используют смартфон.
- Почти 98% детей 11–14 лет имеют собственный смартфон, и большинство используют его ежедневно.
- Время, проведенное онлайн, увеличивается с возрастом: 56% старшеклассников ежедневно проводят в Сети три часа и более, а 20% говорят, что находятся онлайн практически все свободное время.
- В начале 2025 года дети чаще проводили время в мессенджерах и приложениях, представляющих короткие видео. В десятку лидеров по времени использования вошли Telegram, WhatsApp, TikTok и Roblox.
- В 2025 году интерес к чат-ботам на базе ИИ вырос более чем вдвое.

Обучаем и помогаем — детям, родителям и педагогам

Мы считаем, что процесс освоения цифровой грамотности должен быть доступным, понятным и интересным. Поэтому «Лаборатория Касперского» активно участвует в образовательных и просветительских проектах.

- «Урок цифры». В рамках федерального проекта «Урок цифры» в 2025 учебном году мы провели занятия по теме «Кибербезопасность и искусственный интеллект». Школьники, учителя и родители знакомились с базовыми правилами безопасного использования ИИ-технологий, учились распознавать онлайн-мошенничество и узнавали, как специалисты по кибербезопасности используют машинное обучение. Только за первые три недели интерактивные тренажеры были пройдены более 3,5 млн раз.
- «Цифровой ликбез». Для нового сезона всероссийского просветительского проекта «Цифровой ликбез», реализуемого в рамках национального проекта «Экономика данных» и национальной цели «Технологическое лидерство», мы подготовили серию обучающих видеороликов для детей от шести лет. Один из них посвящен проблеме онлайн-груминга, другой — мошенничеству в популярных кликер-играх. Видео рекомендованы для совместного просмотра с родителями или педагогами и сопровождаются методическими материалами, которые можно использовать на уроках, во внеурочной деятельности и при работе с семьями.

Понятные материалы для всей семьи

Чтобы говорить о цифровой грамотности и других сложных вещах простым языком, мы создаем специальные издания для детей и взрослых.

- «Киберазбука» — познавательная книга о мире технологий и цифровых угроз, построенная по принципу алфавита. Она помогает детям и родителям разобраться в новых терминах и научиться безопасному поведению в Сети. В 2024–2025 годах мы перевели книгу на 15 языков, а в октябре 2024 года состоялся коммерческий релиз «Киберазбуки» на русском языке.
- «Цифровой портфель» — практическое пособие для родителей с советами о том, как защитить ребенка как в онлайн-, так и в офлайн-мире: от настройки устройств до бесед о безопасности и доверии. Руководство доступно бесплатно и ориентировано на родителей без технического бэкграунда.

Региональные инициативы

Наша работа по защите детей в интернете выходит далеко за пределы одной страны.

- В **Италии** в рамках Privacy Tour, организованного Итальянским агентством по защите данных, мы передали 500 экземпляров «Киберазбуки» участникам образовательных мероприятий.
- В **Германии** на крупнейшей отраслевой IT-выставке it-sa Expo&Congress в Нюрнберге участники получили 500 таких же книг.
- В **Марокко** наши эксперты приняли участие в семейном дне в школе Cadi Ayad в Касабланке, где рассказали детям и родителям о цифровых рисках и способах защиты от них, а также представили им «Киберазбуку». В мероприятии участвовали порядка 50 детей и их родителей.

KidZania — безопасность через игру и опыт

В марте 2025 года мы открыли Центр киберисследований в детском образовательном парке KidZania Santa Fe в Мексике. Здесь, в известном развлекательном городе, дети в игровой форме знакомятся с основами кибербезопасности, выполняют практические задания и учатся распознавать цифровые риски.

Наши планы на 2026–2027 годы

- Выпуск аналитических отчетов и обучающих материалов по детской онлайн-безопасности
- Участие в образовательных и просветительских проектах для повышения цифровой грамотности среди детей, родителей и педагогов
- Открытие новых центров кибериссследований в детском образовательном парке KidZania в Индии и ОАЭ
- Развитие партнерств с международными правоохранительными организациями, коалициями и НКО, нацеленных на борьбу со сталкингом

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.

Роль ИИ в кибербезопасности

Используя искусственный интеллект и машинное обучение, мы помогаем людям и организациям быстрее распознавать киберугрозы, снижать риски и уверенно пользоваться цифровыми технологиями в повседневной жизни и работе.

Почему это важно

Злоумышленники все активнее используют ИИ для автоматизации атак. Наши эксперты регулярно фиксируют его применение при генерации фишинговых страниц, программ-вымогателей, вредоносного ПО для продвинутых целевых атак (например, Bluenoroff), а также в кампаниях, нацеленных на российские организации, таких как Librarian Likho.

Злоумышленники автоматизируют все больше этапов в цепочке атаки. Однако важно отметить, что ИИ не меняет ландшафт угроз радикально.

ИИ также активно используется в киберзащите: позволяет значительно повысить эффективность обнаружения (детектирования) угроз, включая сложные техники атак, такие как DLL Hijacking[1].

При этом надежная защита по-прежнему строится на многослойном подходе — защите конечных точек и сетей, управляемых сервисах (например, MDR), продвинутых комплексных решениях, таких как XDR, и качественной аналитике угроз (Threat Intelligence). Роль ИИ заключается в другом: он повышает скорость реакции, масштабируемость и точность защитных технологий, помогая противостоять кибератакам.

Как мы используем ИИ в киберзащите

~20 лет

Компания применяет технологии ИИ и ML

135 патентов

в области ИИ в портфеле интеллектуальной собственности «Лаборатории Касперского»

«Лаборатория Касперского» уже почти 20 лет применяет технологии ИИ и машинного обучения (ML) в своих продуктах и сервисах.

Искусственный интеллект помогает ежедневно анализировать сотни тысяч подозрительных и вредоносных файлов, выявляя закономерности и аномалии за доли секунды. При этом мы рассматриваем ИИ не как замену специалистам, а как инструмент поддержки: алгоритмы берут на себя рутинную обработку сигналов, освобождая экспертов для анализа сложных, целевых и нестандартных атак.

Наш центр экспертизы Kaspersky AI Technology Research объединяет исследователей данных, ML-инженеров, экспертов по угрозам и инфраструктуре, чтобы решать самые амбициозные задачи на стыке сфер ИИ/ML и кибербезопасности. Среди этих задач — как разработка и развитие прикладных технологий, так и проведение исследований по безопасности ИИ-алгоритмов, повышение осведомленности о рисках ИИ и многое другое.

Расширяем возможности детектирования угроз

«Лаборатория Касперского» разработала множество ИИ/ML-технологий детектирования угроз, в первую очередь для выявления вредоносного ПО, а также нелегитимной активности злоумышленников. Например, в 2025 году наши эксперты обучили ML-модель выявлять попытки использования техники DLL Hijacking и усилили ей SIEM-систему KUMA. В наших решениях используется не один универсальный алгоритм, а набор специализированных моделей, каждая из которых решает свою задачу. Такой подход делает защиту более устойчивой и точной.

Ключевые направления применения ИИ/ML[2]

- Ранняя проверка файлов. Глубокие нейросети помогают выявлять вредоносные исполняемые файлы по статическим признакам на ранних стадиях, еще до запуска.
- Автоматизация создания правил обнаружения. ML-технологии на базе решающих деревьев помогают формировать правила обнаружения угроз, которые могут работать прямо на устройстве пользователя. Это важно, когда нужно быстро внедрить знания об угрозах в практическую защиту.
- Поведенческий анализ. Даже если файл выглядит безопасным, вредоносная активность может проявиться во время работы программы. Поведенческие модели помогают выявлять такие угрозы по нетипичным действиям.
- Выявление вредоносных интернет-ресурсов на основе анонимной телеметрии, поступающей из установленных у клиентов решений и других источников.
- Защита от фишинга и спама. Специализированные модели, включая ML-модель для детектирования мошеннических веб-страниц и DeepQuarantine для карантина писем с подозрением на спам, снижают риски пользователей.

Благодаря облачной инфраструктуре результаты работы ИИ становятся доступны пользователям почти мгновенно — новые угрозы блокируются сразу после обнаружения.

[1] Техника атаки, при которой злоумышленник внедряет вредоносную динамическую библиотеку (DLL), из-за чего легитимная программа загружает и запускает чужой код.

[2] Подробнее об этих технологиях читайте в документе Машинное обучение для выявления вредоносного ПО.

Боремся с фишингом и онлайн-мошенничеством

Онлайн-мошенничество с годами становится хитрее: современные фишинговые сайты выглядят аккуратно, тексты часто написаны без ошибок, а визуальные элементы копируют интерфейсы известных сервисов. Чтобы противостоять таким угрозам, мы применяем машинное обучение и анализ контента.

В частности, для защиты от фишинга Компания использует:

- технологии оптического распознавания символов (OCR), которые выявляют вредоносный текст, спрятанный внутри изображений;
- собственные запатентованные ML-модели, обученные на массивах легитимных и поддельных сайтов и выявляющие характерные признаки мошенничества.

Это особенно важно, поскольку мошенники все чаще используют изображения и визуальные приманки, пытаясь обойти простые фильтры.

Помогаем специалистам SOC работать эффективнее

В корпоративной среде специалисты по безопасности часто сталкиваются с проблемой избыточного «шума» — большого количества уведомлений, не приводящих к реальным инцидентам. Это приводит к существенным потерям времени.

В сервисах управляемой защиты (Managed Detection and Response) ИИ-алгоритмы автоматически анализируют потоки событий и отфильтровывают ложные срабатывания, позволяя ежегодно закрывать десятки и сотни тысяч неопасных инцидентов без участия человека. В результате специалисты центров мониторинга кибербезопасности (SOC) могут сосредоточиться на действительно важных атаках и быстрее реагировать на реальные угрозы.

В корпоративных решениях для мониторинга и реагирования (Kaspersky SIEM (KUMA) и Kaspersky XDR) риск-скоринг на базе машинного обучения используется для оценки поведения устройств и серверов внутри инфраструктуры. Это помогает выявлять скрытые атаки и аномалии, не передавая данные за пределы компании, что особенно важно для организаций с высокими требованиями к конфиденциальности.

Развиваем ИИ в промышленности и на физических объектах

Искусственный интеллект используется не только для защиты компьютеров и сетей. В промышленности сбои и отклонения могут приводить к простоям, авариям и серьезным финансовым потерям.

Для таких сценариев применяются решения на базе машинного обучения, такие как Kaspersky MLAD (Machine Learning for Anomaly Detection) — программный продукт для предиктивной аналитики. Они анализируют телеметрию оборудования и помогают выявлять ранние (скрытые) признаки надвигающегося отказа оборудования, нарушения техпроцесса, кибератаки, а также ошибки персонала. Постоянно обучая нейросеть, MLAD анализирует поток «атомарных» событий от объекта, структурирует его в паттерны и выявляет нештатное поведение.

Предотвращаем злоупотребление ИИ злоумышленниками

Атакующие активно используют искусственный интеллект для автоматизации своей работы: создания фишинговых ресурсов, ускорения создания вредоносного кода, масштабирования мошеннических схем и создания аудио- и видеодипфейков.

Изучая кейсы обнаруженных угроз, созданных с применением ИИ, наши специалисты улучшают эффективность защиты от вредоносных программ, фишинга и скама, делятся рекомендациями с пользователями. Например, они советуют критически относиться к неожиданным сообщениям, аудио и видео, всегда перепроверять информацию и использовать надежные защитные решения.

Исследуем большие языковые модели

Генеративный ИИ и большие языковые модели уже стали частью цифровой реальности. Мы развиваем инфраструктуру для исследования и безопасного использования их возможностей и быстрого создания прототипов. В этой среде развернуты LLM-инструменты, подобные ChatGPT: они доступны сотрудникам всех подразделений для решения повседневных задач и одновременно служат базой для разработки новых решений.

Одним из ключевых практических сценариев является использование языковых моделей для помощи аналитикам. В частности, сервис Kaspersky Threat Lookup (один из сервисов портала Kaspersky Threat Intelligence Portal) в 2025 году получил ИИ-инструмент для работы с OSINT-данными[1]: алгоритмы анализируют открытые источники и формируют краткую сводку по индикаторам компрометации из всех публикаций, связанных с интересующим объектом. Это позволяет специалистам по информационной безопасности быстрее получать контекст и принимать решения без необходимости вручную изучать большое количество материалов.

[1] Open Source Intelligence — инструменты и возможности для работы с открытыми источниками информации.

Примеры обнаруженных зловредов, созданных с применением ИИ или использующих тему ИИ

- FunkSec. Анализ программы-шифровальщика показал признаки автоматической генерации фрагментов кода; среди целей — организации госсектора, IT, финансов и образования в Европе и Азии.
- RevengeHotels. Новая волна атак на отели с целью кражи данных банковских карт; в кампании выявлены образцы, созданные с применением ИИ.
- Зловреды под видом DeepSeek и Grok. Кампании с поддельными страницами, через которые распространялись стилер, вредоносный PowerShell-скрипт[1] и бэкдор; ссылки на один из зловредных ресурсов размещались в том числе в соцсети X (бывший Twitter).
- BrowserVenom. Фишинговый ресурс, имитирующий сайт DeepSeek, предлагал скачать модель для Windows, а на деле распространял троянец, перехватывающий трафик.
- Jarka. Вредоносные пакеты, распространявшиеся через репозиторий Python Package Index (PyPI) под видом инструментов для чат-ботов на основе нейросетей, заражали устройства стилером.
- Gipy. Загрузчик распространялся под видом приложения на основе нейросетей для изменения голоса.

[1] Скрипт для среды PowerShell, применяемый злоумышленниками для скрытого выполнения команд, загрузки вредоносного кода или управления зараженной системой.

[2] Способ манипулирования ИИ, при котором инструкции для модели скрыто встраиваются в данные, с которыми она работает, а не передаются ей напрямую.

Наши исследования по теме ИИ

Как нейросети выдают мошенников:

мы проанализировали артефакты, которые LLM могут оставлять на фишинговых и скам-страницах (включая характерные фразы и следы в разметке).

Для чего и как люди манипулируют нейросетями:

выяснили, как и для чего люди используют непрямые инъекции затравки[2], — например, чтобы обратить внимание больших языковых моделей на свои резюме и т. д.

Услуги по созданию видео- и аудиодипфейков в режиме реального времени:

проанализировали предложения на теневых площадках и типовые сценарии злоупотреблений.

Как мы управляем безопасностью ИИ

Мы рассматриваем безопасность ИИ как комплексную задачу, которая выходит далеко за рамки самих технологий. Речь идет не только о защите алгоритмов и моделей, но и о том, как ИИ используется внутри Компании, какие данные с ним работают, какие риски это создает и как построено управление этими рисками.

Вопросы безопасности ИИ затрагивают сразу несколько направлений:

- юридические и правовые аспекты — например, какие данные допустимо использовать и передавать в облачные ИИ-сервисы;
- IT- и ИБ-процессы, в том числе управление доступами, контроль конфигураций и предотвращение использования так называемого «теневого ИИ», когда сотрудники применяют внешние ИИ-инструменты без согласования;
- процессы разработки и обучения моделей, где важно понимать источники данных, возможные искажения, уязвимости моделей и сценарии их некорректного использования.

Для эффективного управления этими рисками требуется участие специалистов из разных областей — информационной безопасности, IT, юридических команд, а также экспертов по данным (data science) и машинному обучению. В идеальной модели необходимы отдельные специалисты по безопасности ИИ, координирующие работу этих команд.

Мы также учитываем, что область безопасности ИИ развивается очень быстро. Постоянно появляются новые подходы, уязвимости, методы атак и инструменты защиты. Поэтому мы рассматриваем управление рисками ИИ как непрерывный процесс, который требует регулярного обновления знаний, практик и обучающих материалов.

Развиваем сотрудничество и делимся экспертизой

Экспертиза «Лаборатории Касперского» в области ИИ формируется системно — от фундаментальных исследований и инфраструктуры обучения моделей до практического применения в продуктах и сервисах. Мы исходим из того, что устойчивый прогресс в развитии ИИ возможен только при активном обмене знаниями. Поэтому Компания участвует в международных инициативах и отраслевых альянсах, сотрудничает с профессиональным и академическим сообществом и присутствует в профильных рейтингах.

В 2024 году «Лаборатория Касперского» стала участником Глобального альянса по искусственному интеллекту для промышленности и производства (AIM Global), созданного в 2023 году. Альянс объединяет правительства, международные организации, коммерческие компании и отраслевых лидеров. Участие в AIM Global позволяет обмениваться экспертизой, участвовать в формировании единых подходов к применению ИИ и поддерживать развитие технологий с учетом этических, социальных и технологических аспектов.

В 2025 году Компания присоединилась к числу организаций, поддерживающих концепцию Глобального цифрового договора ООН. В документе перечислены задачи и принципы, которые будут способствовать достижению инклюзивного, открытого и устойчивого цифрового будущего.

Мы делимся с сообществами своей экспертизой в сфере ИИ. Некоторые исследования, например о монотонных алгоритмах машинного обучения или применении нейросетей к детектированию спама, выходят в формате академических статей на ведущих конференциях по машинному обучению, другие — на специализированных порталах и ИБ-конференциях.

Так, мы публикуем исследования безопасности собственных ИИ-алгоритмов — в том числе пишем о смоделированных атаках на алгоритмы детектирования спама и вредоносного ПО. Исследуем использование нейронных сетей для анализа временных рядов.

Кроме того, мы выпускаем обучающие материалы и курсы, в том числе для специалистов по информационной безопасности и разработчиков, чтобы помочь им безопасно внедрять ИИ-решения и учитывать возможные риски.

В 2025 году «Лаборатория Касперского» выпустила курс по обучению разработчиков и специалистов по информационной безопасности основам безопасности систем на базе больших языковых моделей. Также мы постоянно обновляем портфолио тренингов для экспертов, чтобы учебные материалы соответствовали потребностям бизнеса, государственных и научных учреждений.

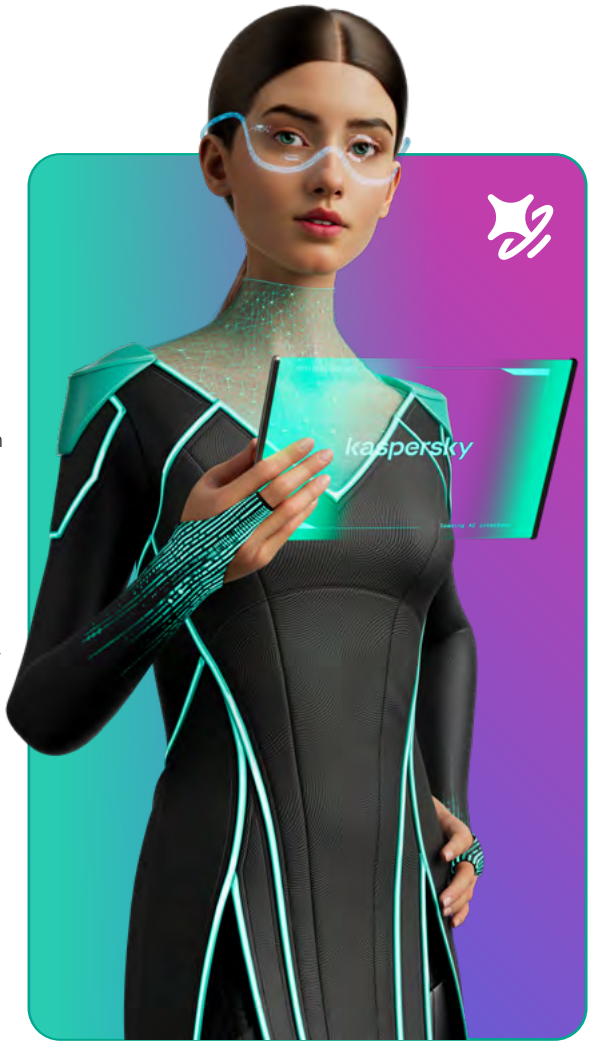
Kaspersky Unified Monitoring and Analysis Platform

Экспертиза «Лаборатории Касперского» в области ИИ и ML подтверждается и внешним признанием. В 2025 году Компания стала победителем премии «ИТ-Лидер» в номинации «Искусственный интеллект». Награды была удостоена SIEM-система Kaspersky Unified Monitoring and Analysis Platform (KUMA) со встроенным ИИ-ассистентом Kaspersky Investigation and Response Assistant (KIRA).

ИИ-ассистент KIRA был внедрен в платформу в конце 2024 года. В его основе лежит нейросетевая модель «ГигаЧат», разработанная Сбером. Ассистент помогает анализировать события информационной безопасности, снижая нагрузку на специалистов, сокращая объем рутинных операций и уменьшая вероятность ошибок при интерпретации инцидентов.

Smart Ranking

Также в 2025 году «Лаборатория Касперского» заняла пятое место в российском рейтинге SmartRanking в области ИИ, продемонстрировав заметный рост выручки от продаж решений с использованием ИИ и машинного обучения. А в 2024 году компания была признана одним из ключевых работодателей в сфере ИИ в России по результатам исследования TAdviser.



Следуем принципам ответственного и этичного использования ИИ

Мы убеждены, что искусственный интеллект должен использоваться ответственно и прозрачно, особенно в такой чувствительной сфере, как кибербезопасность. Поэтому Компания регулярно участвует в разработке законодательных актов, создании политик и других документов, охватывающих разные аспекты безопасности в работе с новыми технологиями, в том числе ИИ.

В рамках Форума ООН по управлению интернетом в 2024 году «Лаборатория Касперского» представила руководство по безопасной разработке и внедрению систем на основе ИИ.

Ранее, в 2023 году, мы сформулировали и публично представили на Internet Governance Forum первые принципы этичного использования ИИ в кибербезопасности, которых придерживаемся в своей работе.

- **Прозрачность.** Объясняем, как работает ИИ — клиенты имеют право понимать, где и зачем используются технологии машинного обучения.
- **Безопасность.** Делаем безопасность приоритетом — все ИИ-системы проходят проверки, тестирование и специальный аудит. Принимаются меры по минимизации зависимости от сторонних наборов данных в процессе обучения ИИ-решений.
- **Человеческий контроль.** Специалисты всегда могут вмешаться, проверить и скорректировать работу алгоритмов при анализе сложных угроз.
- **Конфиденциальность.** Принимаем меры для защиты данных и систем, чтобы обеспечить цифровую приватность клиентов.
- **Приверженность целям кибербезопасности.** Сосредоточившись исключительно на защитных технологиях, мы следуем своей миссии строить более безопасный мир и демонстрируем приверженность защите пользователей и их данных.
- **Открытость к диалогу.** Обмениваемся передовым опытом в области этичного использования алгоритмов машинного обучения со всеми заинтересованными сторонами.

Планы на 2026–2027 годы

Компания планирует и дальше развивать портфель решений на базе машинного обучения, дополняя его технологиями, которые охватывают полный цикл работы с решениями по кибербезопасности. Наш подход основан на принципе разумной достаточности: мы используем максимально надежные и быстрые методы ИИ, но при этом — эффективные и понятные.

В числе приоритетных планов:

- развитие классических статистических и ML-моделей для детектирования разных видов вредоносного ПО, контентных атак и аномалий — в том числе для поиска атак, связанных с боковым перемещением и несанкционированным использованием учетных записей;
- применение генеративного ИИ для новых классов задач, недоступных традиционным ML-алгоритмам, в первую очередь через расширение навыков ассистента KIRA и применение его в разных продуктах — от Kaspersky SIEM до Kaspersky Container Security;
- развитие агентной парадигмы: создание навыков KIRA, которые комбинируют существующие функции решений и помогают в многошаговых сценариях расследования и реагирования без заранее заданного сценария. Такая глубокая интеграция может потребовать создания интерфейсов MCP (Model Context Protocol), для организации доступа ИИ-модели к встроенным инструментам наших решений;
- выход на рынок решений по управлению уязвимостями (Vulnerability Management). Новый продукт, усиленный технологиями ИИ, поможет организациям своевременно выявлять и устранять уязвимости и ошибки конфигурации в IT-инфраструктуре.

Люди в «Лаборатории Касперского»

~5,7 тысячи
сотрудников работают в «Лаборатории Касперского»

18%
сотрудников работают в Компании больше 10 лет

197,1 млн
рублей потрачено на обучение сотрудников в 2024–2025 годах

Управление персоналом

GRI 3-3

Сотрудники — главная ценность нашей Компании. Мы стремимся сделать работу в «Лаборатории Касперского» комфортной и интересной, чтобы каждый мог быть продуктивным, чувствовать себя защищенным, развиваться и развивать Компанию.

~1000

сотрудников присоединилось в 2025 году

В том числе

>200 стажеров

13%

российских сотрудников выросли в Компании со стажерской позиции, включая двух топ-менеджеров

Ключевые документы

- Трудовой кодекс Российской Федерации
- Правила внутреннего трудового распорядка
- Положение о выплатах компенсационного порядка
- Положение об оплате труда
- Политика в отношении обработки персональных данных

Наш подход к управлению персоналом

Мы выстраиваем отношения с сотрудниками на основе доверия и взаимного уважения. Наш подход заключается в постоянном анализе рабочих процессов и рабочей среды, в которой они находятся. Мы стремимся слышать их потребности и поддерживать в любых ситуациях, что помогает создавать необходимые условия для продуктивной работы и развития персонала и, как следствие, для развития бизнеса в целом.

Наши ключевые задачи:

- обеспечение достойных условий труда и развития, включая конкурентное вознаграждение и широкий соцпакет;
- инвестиции в обучение и развитие сотрудников, внедрение новых образовательных программ;
- создание условий для карьерного роста, расширения профессионального опыта или смены карьерного пути сотрудников.

Система управления персоналом

Работой с персоналом занимается профильный департамент, который включает восемь направлений. Каждое из них узко специализируется на конкретных задачах. Разделение зон ответственности помогает структурировать управление персоналом и адаптировать его для крупного международного бизнеса. В частности, структура предусматривает отдельное направление, ассоциированное с международной деятельностью.

Помимо этого, «Лаборатория Касперского» рассматривает развитие и инвестиции в персонал как отдельную важную функцию и ряд направлений занимается именно этими вопросами.

Корпоративная культура и деловая этика

Мы придерживаемся высоких стандартов управления и деловой этики с помощью внедрения лучших корпоративных практик. Корпоративная культура «Лаборатории Касперского» поддерживает развитие сотрудников, их карьерный рост и личное благополучие.

Ключевые документы

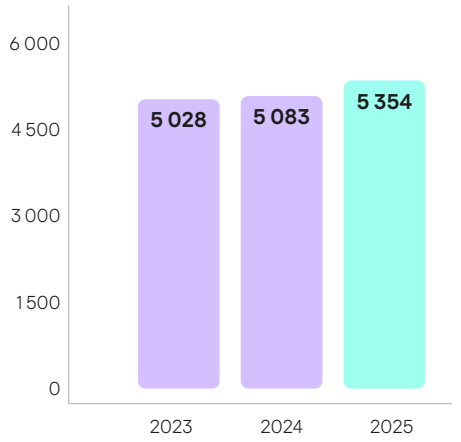
- Трудовой кодекс Российской Федерации
- Этический кодекс Компании
- Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН

Численность и структура персонала

GRI 2-7, GRI 401-1, СОКБ 21, СОКБ 34

В 2025 году общая численность сотрудников «Лаборатории Касперского» выросла на 11,3% год к году и достигла 5 691 человека.

Среднесписочная численность сотрудников Компании[1], человек



В 2025 году к нам присоединилось около 1000 новых сотрудников, в том числе более 200 стажеров. При этом 18% сотрудников работают в «Лаборатории Касперского» больше 10 лет, а 13% российских сотрудников выросли в Компании со стажерской позиции, включая двух топ-менеджеров.

В 2025 году мы отмечаем значительное снижение уровня текучести персонала — на 5 п. п., до 10% с 15% годом ранее. «Лаборатория Касперского» обеспечивает непрерывность бизнеса по линии HR, внедряет новые HR-практики и улучшает текущие. Мы верим в долгосрочные отношения с людьми и в развитие возможности для их роста внутри Компании. Кроме того, важную роль в удержании талантов играют интересные и амбициозные задачи, а также команда экспертов и общая корпоративная культура.

+11,3%

рост общей численности сотрудников в 2025 году по сравнению с 2024 годом

[1] Показатель за 2023 год был скорректирован относительно ранее опубликованных данных в связи с изменением методики расчета.

Наша система мотивации

«Лаборатория Касперского» создает комфортную и мотивирующую среду, в которой сотрудники чувствуют поддержку, видят возможности для роста и понимают ценность своего вклада.

Мы внимательно относимся ко всем аспектам рабочей жизни — от условий в офисе до оценки результатов. Мы уверены, что вклад квалифицированных специалистов в развитие Компании должен вознаграждаться, поэтому мы поддерживаем конкурентный уровень заработной платы, предлагаем сотрудникам один из самых широких соцпакетов на рынке, активно внедряем и совершенствуем программы развития и обучения.

Ежегодно в Компании проходит процесс пересмотра заработных плат. В 2025 году заработная плата сотрудников «Лаборатории Касперского» была увеличена в среднем на 19%.

Материальная мотивация

Мы стремимся обеспечить сотрудникам высококонкурентную и справедливую оплату, которая помогает привлекать и удерживать лучших специалистов и мотивировать их на достижение результатов.

При построении программ вознаграждения мы руководствуемся следующими принципами.

1. **Вознаграждение за результаты.** В Компании нет понятия индексации заработной платы, но есть ежегодный процесс пересмотра заработных плат. Это позволяет поддерживать конкурентоспособность заработной платы сотрудников и ускорять рост тех, кто показывает высокую результативность.
2. **Внешняя конкурентоспособность.** Мы регулярно изучаем рынок и следим за тем, чтобы наше предложение по совокупному вознаграждению оставалось высококонкурентным.
3. **Прозрачность.** Мы открыто рассказываем сотрудникам о подходах к формированию пакета вознаграждения, чтобы обеспечить понимание нашей философии вознаграждения.

В Компании целевое совокупное вознаграждение (Total Target Cash Compensation, TTCC) включает фиксированную часть (оклад) и целевой бонус.

В 2024 году заработная плата сотрудников «Лаборатории Касперского» в России выросла в среднем на 15% год к году, а в 2025 году рост составил в среднем 19%.

Среднее повышение заработной платы сотрудников Компании по сравнению с предыдущим годом

15%	19%
в 2024 году	в 2025 году

Социальная политика и забота о людях

GRI 401-2

Мы поддерживаем сотрудников на протяжении всего периода работы в Компании и делаем все возможное, чтобы люди могли чувствовать себя уверенно в разных жизненных ситуациях.

В России соцпакет доступен всем сотрудникам[1] и включает в том числе:

- добровольное медицинское страхование (ДМС) со стоматологией (в том числе для детей сотрудников до 16 лет включительно);
- доплату до 100% оклада к листку нетрудоспособности до 15 рабочих дней в год;
- доплату до 100% оклада к листку нетрудоспособности по беременности и родам на весь период;
- ведение беременности и родов;
- выплату при рождении ребенка;
- участие в программе лечения онкологии в России;
- материальную помощь в случае смерти близкого родственника и в других сложных жизненных ситуациях;
- страхование от несчастного случая;
- страхование выезжающих за рубеж;
- релокационную выплату при переезде в Москву;
- комфортный и зеленый офис класса «А»;
- премии юбилярам (по достижении 50, 60, 70 лет) и бонусы сотрудникам, стаж которых в Компании достиг 10 и 25 лет;
- компенсацию стоимости занятий спортом;
- изучение иностранных языков.

Сотрудники могут прямо в офисе воспользоваться услугами врача-терапевта, массажистов и психолога, посещать спортивные залы и сауну. Для них также создана линия психологической поддержки онлайн. Кроме того, Компания развивает корпоративные спортивные программы и компенсирует сотрудникам расходы на занятия фитнесом.

Регулярные внутренние коммуникации помогают нам узнавать мнение сотрудников по поводу различных аспектов работы: мы проводим AMA-сессии и Kick-off-встречи[2] с руководством, делимся результатами и планами, обсуждаем стратегию. Ежегодно оцениваем уровень удовлетворенности сотрудников работой посредством внутреннего опроса, а также проводим церемонию Annual Kaspersky Awards, где отмечаем главные личностные и командные достижения всех подразделений.

Мы помогаем всем сотрудникам, в чьих семьях появляются дети, — как родителям, так и усыновителям или опекунам. Им предоставляется отпуск по уходу за ребенком, а к государственному пособию по беременности и родам добавляется корпоративная доплата до полного оклада на протяжении всего отпуска по беременности и родам (как правило, 140 календарных дней).

Подробнее о поддержке матерей с детьми читайте в подразделе «Поддерживаем родительство и благополучие сотрудниц», на с. 65

Карьерное развитие и стажировки

Мы видим развитие людей как основу развития бизнеса. Компания поощряет карьерные перемещения — как вертикальные, так и горизонтальные, — между должностями, командами и направлениями. Это помогает расширить опыт сотрудников, улучшает взаимодействие между подразделениями и повышает мотивацию.

В отчетном периоде мы запустили ряд инициатив, направленных на поддержку карьерного роста:

- **Grow Lab** — пространство для обмена знаниями и развития экспертизы, где сотрудники могут учиться друг у друга и работать с наставниками;
- **Internal Mobility** — программа, направленная на развитие практики внутренних переходов, которая помогает сотрудникам пробовать себя в новых ролях и проектах внутри Компании, если они готовы к этому;
- **карьерные консультации** — индивидуальная поддержка сотрудников при выборе дальнейших шагов в развитии: от углубления текущей экспертизы до смены направления.

Особое внимание мы уделяем молодым специалистам. С 2016 года в Компании работает программа оплачиваемых стажировок для студентов Kaspersky SafeBoard. Порядка половины стажеров переходят в штат по окончании стажировки. Многие из них сегодня занимают руководящие позиции разных уровней и уже сами подбирают стажеров в свои команды через программу SafeBoard.

Подробнее о программе SafeBoard читайте в подразделе «Подготовка кадров для IT-отрасли», на с. 86

[1] Для сотрудников с временными трудовыми договорами и работающих на условиях неполной занятости доступен сокращенный соцпакет. В Компании около 0,1% таких сотрудников.
[2] Установочная встреча.

Равные возможности

СОКБ 56

«Лаборатория Касперского» обеспечивает всем сотрудникам равные возможности и не допускает дискриминации в любых ее проявлениях.

Это один из наших ключевых корпоративных принципов, который соответствует одобренным ООН Руководящим принципам предпринимательской деятельности в аспекте прав человека, а также Целям устойчивого развития ООН, включая ЦУР 4.5, 5.1 и 8.5.

Подробнее о вкладе Компании в достижение ЦУР ООН читайте в разделе «Устойчивое развитие» на с. 20

Мы строго соблюдаем требования законодательства и принимаем решения о найме, развитии и вознаграждении сотрудников исключительно на основе их профессиональных качеств, опыта и достижений — без ограничений по полу, возрасту или другим признакам.

Уважение и безопасная рабочая среда

Принятые в Компании правила и стандарты поведения основаны на ценностях и принципах «Лаборатории Касперского». Каждый сотрудник важен для Компании и заслуживает уважения. Мы стремимся поддерживать здоровую, открытую и доброжелательную рабочую атмосферу, в которой людям комфортно сотрудничать, делиться идеями, развиваться.

В Компании недопустимы любые формы дискриминации, унижения достоинства, оскорблений, какого-либо давления и нарушения личных границ. Мы придерживаемся общепринятых норм деловой этики и ожидаем от сотрудников и партнеров профессионального, корректного и уважительного поведения.

Как мы поддерживаем сотрудников

Мы выстраиваем отношения внутри Компании на основе доверия и взаимного уважения. Чтобы рабочая обстановка оставалась комфортной для всех, мы регулярно анализируем условия труда, процессы оценки эффективности и обратную связь от сотрудников. Мы слышим потребности каждого и делаем все, чтобы сотрудники «Лаборатории Касперского» чувствовали поддержку и заботу в любой ситуации.

В Компании в рамках HR действует функция бизнес-партнерства. HR-бизнес-партнеры помогают выстраивать диалог между бизнесом и сотрудниками, поддерживают команды в сложных ситуациях и способствуют поиску решений, учитывающих интересы всех сторон.

Если сотрудник сталкивается с проявлениями дискриминации или неэтичного поведения, он может сообщить об этом команде HR Support или своему HR-бизнес-партнеру. Кроме того, команда HR Support всегда готова помочь сотрудникам с любыми вопросами — от административных процедур до консультаций по корпоративному обучению и развитию.

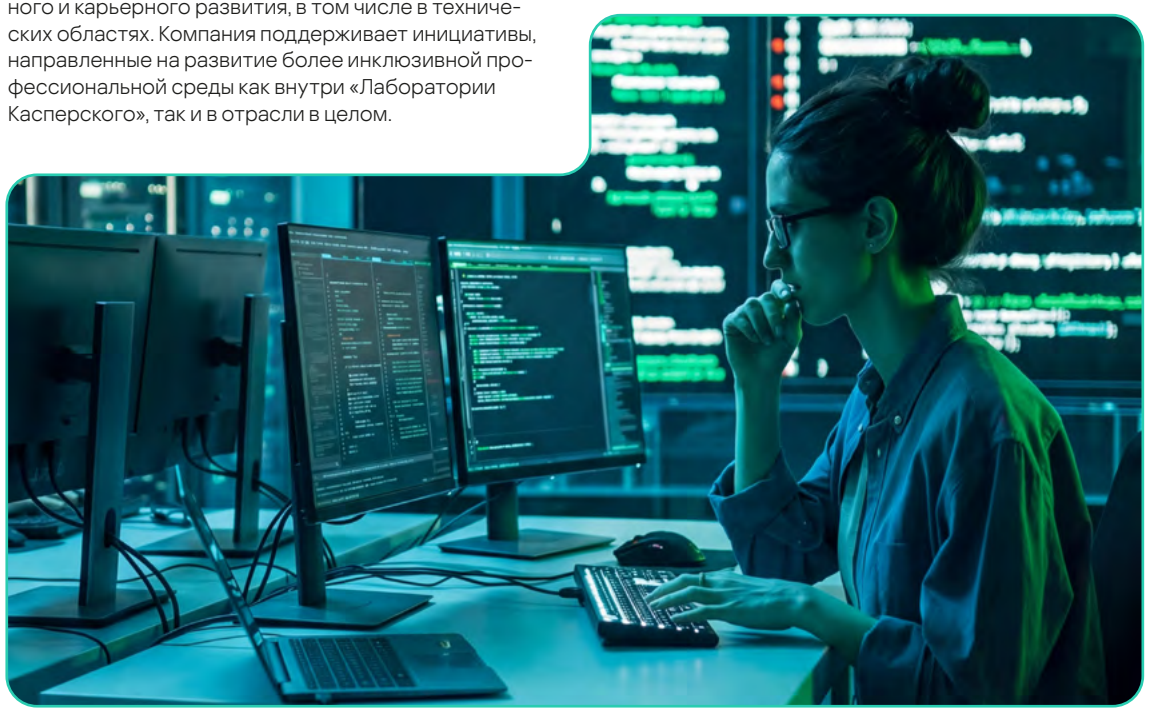
Женщины в IT

«Лаборатория Касперского» последовательно работает над тем, чтобы показывать разнообразие карьерных возможностей в IT и создавать среду, в которой люди с разным опытом и профессиональным путем, разделяющие ценности Компании, могут реализовать свой профессиональный потенциал. Такая работа ведется на разных рынках присутствия Компании по всему миру.

Особое внимание уделяется преодолению устойчивых стереотипов о роли женщин в технологической сфере и расширению возможностей для их профессионального и карьерного развития, в том числе в технических областях. Компания поддерживает инициативы, направленные на развитие более инклюзивной профессиональной среды как внутри «Лаборатории Касперского», так и в отрасли в целом.

Наш подход к поддержке женщин

Мы убеждены, что устойчивые инновации возможны только в той среде, где у всех сотрудников, независимо от пола, есть равный доступ к возможностям, поддержке и признанию. Наши инициативы — это часть долгосрочной стратегии, направленной на формирование более безопасного и инклюзивного цифрового мира благодаря разнообразию опыта и точек зрения команд, в которых присутствуют как мужчины, так и женщины. Таким мы видим будущее в сфере IT и кибербезопасности — разнообразное и основанное на силе разных голосов.



Начинаем со школ и университетов

Мы заботимся о том, чтобы с ранних лет делать IT-образование доступным и открытым для всех. Для этого Компания сотрудничает со школами и университетами по всему миру, проводит лекции, мастер-классы и программы стажировок, чтобы все школьники и студенты вне зависимости от их пола могли лучше понять технологическую сферу и увидеть собственный потенциал в IT и кибербезопасности.

Развиваем женское IT-сообщество внутри Компании

Вовлечение женщин в IT-индустрию и их поддержка — важная часть корпоративной культуры «Лаборатории Касперского», которая формируется на уровне совета директоров и высшего менеджмента. При этом женщины, уже достигшие успеха на различных уровнях, активно участвуют в программах поддержки: общаются с коллегами и подчиненными, делятся опытом и своим примером вдохновляют начинающих IT-специалистов.

Помимо этого, мы поддерживаем внутреннее женское IT-сообщество и инициативы, направленные на расширение представительства женщин в технологических и смежных ролях.

Обеспечиваем равный доступ к карьерным возможностям

«Лаборатория Касперского» стремится быть максимально честной и открытой, чтобы не допускать проявлений гендерной дискриминации.

При подборе новых сотрудников для нашей команды мы придерживаемся skills-based-подхода: нас интересуют прежде всего профессиональные навыки, квалификация и релевантный опыт кандидатов. Мы оцениваем компетенции независимо от пола, уделяя внимание мотивации и тому, насколько кандидат разделяет ценности Компании и готов вносить вклад в общую миссию. Такой подход помогает минимизировать риск дискриминации и поддерживать честную и прозрачную систему отбора.

25%

доля сотрудников-женщин в «Лаборатории Касперского»

26,7%

доля женщин в мировой технологической отрасли в 2025 году[1]

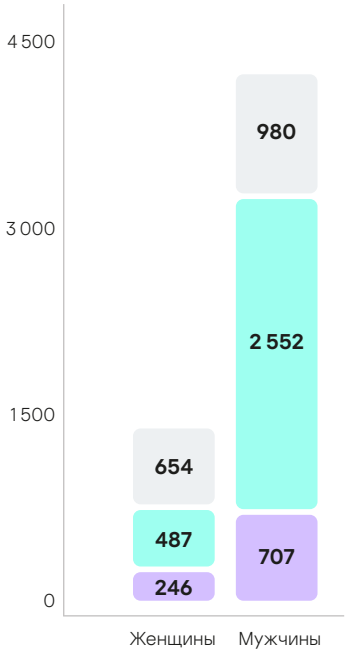
26%

женщин на руководящих позициях в Компании

[1] По данным исследования Exploding Topics. К технологическому сектору (tech) относятся компании, работающие в сфере IT, кибербезопасности, ИИ, облачных технологий и др.

SASB TC-SI-330a.3

Общая численность сотрудников в разбивке по полу и категориям в контексте гендерного баланса[1], человек

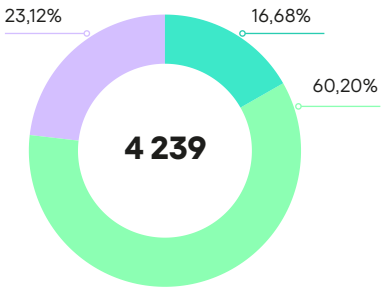


- Руководители[2]
- Технические специалисты
- Прочие специалисты

GRI 405-1

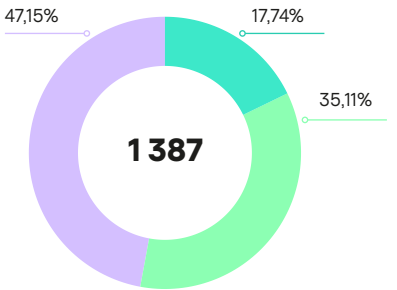
Сотрудники Компании в разбивке по гендеру и категориям[3], человек

Мужчины



Руководители[2]	707
Технические специалисты	2 552
Прочие специалисты	980

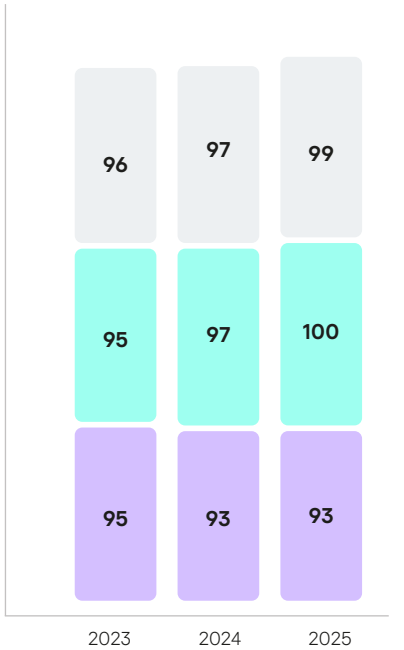
Женщины



Руководители	246
Технические специалисты	487
Прочие специалисты	654

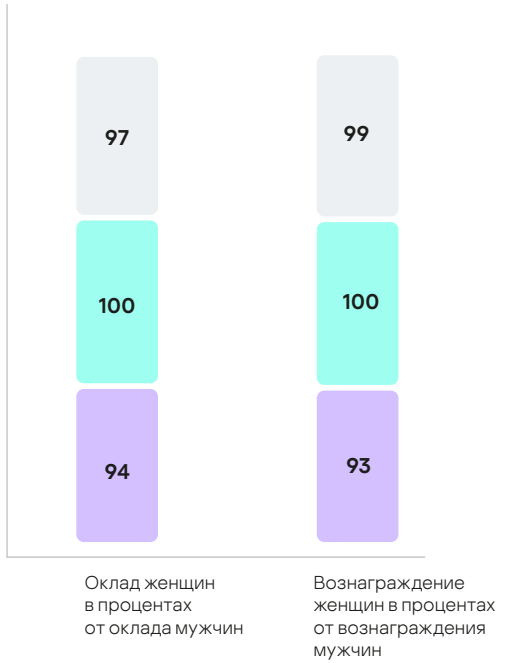
GRI 405-2

Соотношение совокупного вознаграждения[4] женщин и мужчин[5], %



- Руководители[2]
- Технические специалисты
- Прочие специалисты

Соотношение оклада[6] и совокупного вознаграждения[4] женщин и мужчин[1] в 2025 году, %



- Руководители[2]
- Технические специалисты
- Прочие специалисты

1 Данные указаны по московскому офису Компании на 31 декабря 2025 года.
2 Менеджеры, у которых в подчинении от одного человека.
3 На 31 декабря 2025 года.
4 Целевое совокупное вознаграждение состоит из оклада и целевого бонуса.
5 Данные указаны по московскому офису Компании на конец года.
6 Оклад — это фиксированная и гарантированная часть вознаграждения сотрудников.

Поддерживаем родительство и благополучие сотрудниц

СОКБ 43

Во всех странах нашего присутствия мы стараемся вдохновлять сотрудниц на их карьерном пути и поддерживать в самые важные моменты жизни. Например, в России сотрудницам, у которых в семье происходит пополнение, мы предлагаем:

- программу ведения беременности и родов по ДМС;
- отпуск по уходу за ребенком, который может взять любой из родителей, независимо от того, родной это ребенок, усыновленный или находящийся под опекой;
- 100%-ную доплату к государственному пособию по беременности и родам, чтобы общая сумма выплат достигала полного размера оклада, — ее получают сотрудницы, имеющие стаж работы в Компании не менее одного года;
- единовременную материальную помощь при рождении ребенка: 150 000 рублей за первого ребенка и 200 000 рублей при рождении второго и последующих детей;
- ежегодно частичную компенсацию расходов сотрудников на приобретение путевок в летние лагеря для их детей в размере 50% от стоимости путевки;
- страховку для детей до 16 лет включительно в рамках ДМС.

Объединяем женщин в онлайн-сообщества

В 2021 году «Лаборатория Касперского» запустила глобальный проект Empower Women — онлайн-платформу о женщинах в сфере кибербезопасности и технологий, которая объединяет исследования по различным регионам, новости и вдохновляющий подкаст Women in IT с участием сотрудниц Компании. За отчетный период на сайте появились десять новых рассказов о наших коллегах из разных стран, в которых они делятся историями своего профессионального и личного развития, четыре обзора мнений и шесть спецпроектов. Мы стремимся показать широкий спектр возможностей построения карьеры в IT-индустрии — многие героини добились высоких результатов в разных областях внутри IT-компании, будь то разработка, продажи, образовательные проекты или коммуникации.

В 2024 году появился проект «Вам письмо!», где наши сотрудницы делятся личными и профессиональными историями в формате писем самим себе в юности, рассказывая о преодоленных трудностях и уроках, которые помогли им стать теми, кто они есть сейчас. Эти откровенные истории вдохновляют будущие поколения женщин в IT и поддерживают тех, кто находится в начале пути или переживает сложные решения в карьере и жизни.

Спецпроекты о женщинах в технологиях

«Лаборатория Касперского» реализует ряд глобальных тематических проектов, посвященных роли женщин в технологической истории и сегодняшнем дне IT-отрасли.

Среди инициатив 2025 года — проект Women in the History of Tech, который рассказывает о женщинах, внесших вклад в развитие технологий в самых разных сферах — от кибербезопасности, IT-предпринимательства и цифрового образования до телекоммуникаций, государственной цифровой политики, электронной коммерции и общественной безопасности. Участницами проекта стали женщины-профессионалы с опытом работы в технологическом бизнесе, стартап-среде, государственном секторе и образовательных инициативах, демонстрирующие разнообразие карьерных траекторий в цифровой индустрии.

Еще одна инициатива — Mothers in Tech, посвященная сотрудницам Компании, которые совмещают профессиональную карьеру и материнство. Проект показывает, что успешная самореализация может иметь разные формы и строиться с учетом индивидуальных жизненных обстоятельств и приоритетов.

В этом же году появился еще один новый проект — интерактивная тест-игра Confronting IT's Career Barriers, которая показывает, с какими препятствиями сталкиваются специалисты в технологических сферах. Участники делают выбор, какие барьеры они готовы терпеть, и узнают, как такие компромиссы могут тормозить рост и почему их нельзя игнорировать. Тестирование также дает рекомендации, как преодолеть эти барьеры, и объясняет, какое значение они имеют для технологического сектора.

Всего в тесте участвовали более 400 мужчин и женщин со всего мира. Они помогли выявить наиболее болезненные препятствия, в число которых вошли токсичная или нездоровая рабочая среда, переработки, ограниченные возможности для карьерного роста, недостаточно прозрачные критерии продвижения и предвзятость в оценке сотрудников. Полученные результаты демонстрируют важность изменений в корпоративной культуре.

Вдохновляем новое поколение женщин в IT

Чтобы помочь будущему поколению женщин в технологиях, «Лаборатория Касперского» запустила глобальную инициативу Future You in Tech — тест-игру, ориентированную на школьниц и студенток, которые выбирают свой карьерный путь. Проект помогает девушкам понять, что включает в себя сфера кибербезопасности, какие роли и карьерные возможности она открывает и какие из них могут подойти им с учетом личных интересов и талантов, а также снижает барьеры входа в профессию.

В 2025 году мы активно продвигали проект на международной арене: совместно с Africaines in Tech представили тест на саммите Transform Africa Summit, организованном Smart Africa в Конакри (Гвинея), и на онлайн-сессии Women in Tech Special конференции ATDA[1] в Рабате (Марокко). Это позволило привлечь больше молодых женщин из стран Африки, рассматривающих карьеру в IT. На момент подготовки Отчета в тесте приняли участие более 180 юных девушек, и эта цифра продолжает расти по мере расширения географии инициативы.

[1] ATDA — Assises de la Transformation Digitale en Afrique, крупное отраслевое мероприятие по цифровой трансформации в Африке.

Партнерства, мероприятия и активности

«Лаборатория Касперского» выстраивает долгосрочные партнерства и активно участвует в инициативах, которые помогают укреплять позиции женщин в IT и кибербезопасности по всему миру. В нашем фокусе — поддержка карьерного роста, развитие лидерства, обмен опытом и расширение доступа к цифровым возможностям для женщин и девушек.

В 2024 году Компания выступила спонсором проекта 100 Women Face to Face. В рамках инициативы прошли офлайн- и онлайн-встречи, а также серия вебинаров о развитии карьерного потенциала женщин в технологиях. Дополнительно в журнале BT Haber была опубликована вступительная колонка генерального директора «Лаборатории Касперского» в Турции Илкем Озар, в которой она рассказала о целях и значении проекта.

Журнал CIO Update (Турция) посвятил специальный выпуск к 8 Марта женщинам-лидерам в IT. Генеральный директор «Лаборатории Касперского» в Турции Илкем Озар участвовала в групповом фото на обложке вместе с ведущими женщинами рынка и дала интервью для печатной и видеоверсии, рассказав о своем карьерном пути и важности инклюзии в технологической сфере.

В марте 2024 года в Мексике «Лаборатория Касперского» провела пресс-конференцию, посвященную представлению отчета State of Stalkerware и повышению осведомленности о проблеме цифрового сталкинга. В дискуссии приняли участие известная правозащитница в сфере цифровых прав Олимпия Корал и менеджер по потребительским продуктам «Лаборатории Касперского» в Мексике Джудит Тапия. Спикеры обсудили влияние сталкерского ПО на пользователей и представили практические рекомендации по его выявлению и предотвращению.

В рамках летнего учебного лагеря для 800 студентов из разных турецких университетов, организованного учебными заведениями и центрами BUSIBER Bogazici University MIS Cybersecurity Center и Cyber Technology Clubs, «Лаборатория Касперского» провела обучающий день и панель Women in Technology, посвященную растущей роли женщин в кибербезопасности. Модератором выступила генеральный директор «Лаборатории Касперского» в Турции Илкем Озар, а приглашенные отраслевые эксперты обсудили, как укрепить позиции женщин в IT и какие карьерные возможности открываются для них.

Руководитель направления мониторинга цифровых угроз в «Лаборатории Касперского» Анна Павловская выступила на форуме European Women in Tech. Она представила свое исследование о психологических портретах киберпреступников, основанное на изучении неформальных диалогов участников даркнет-форумов.

Старший менеджер по связям с государственными структурами «Лаборатории Касперского» Глэдис Ядом приняла участие в мероприятии Future Forward Paris, организованном проектом Wonder Women Tech. В рамках панельной дискуссии «Воздействие и устойчивость: строим лучшее будущее» она рассказала, как Компания помогает делать мир безопаснее с помощью образовательных проектов для уязвимых групп и инициатив, направленных на поддержку женщин.

Компания выступила партнером по экспертизе на конференции Women Empowerment Conference (WEC) в Западной Африке, объединяющей женщин-лидеров, предпринимательниц и инноваторов в сфере технологий из разных стран региона. Мероприятие было посвящено вопросам инклюзии, лидерства и расширения доступа женщин к цифровым возможностям.

В 2025 году Компания подписала трехлетнее Соглашение о взаимопонимании (MoU) с проектом Smart Africa. Это важное партнерство нацелено на развитие кибербезопасности по всему африканскому континенту и сокращение гендерного разрыва в STEM/ICT за счет специальных программ для женщин и девушек.

В 2024–2025 годах сотрудники «Лаборатории Касперского» выступали наставниками, проводили вебинары и предоставляли бесплатный доступ к обучению для стажеров программы Outreachy и других начинающих специалистов. Эти активности помогают молодым профессионалам, включая женщин, получить первые навыки и опыт в IT и кибербезопасности.

В июле 2025 года совместно с сообществом Women in Tech Russia была организована онлайн-конференция «Как проявить себя в IT: личный бренд и digital-репутация для карьерного роста». В первой части прошел круглый стол «Как формируется образ IT-специалиста в глазах нанимателей — от GitHub до LinkedIn, от старых форумов до конференций» с участием директора управления по привлечению и развитию талантов «Лаборатории Касперского» Елены Михеевой. Во второй части состоялись выступления в формате TED Talks, включая доклад руководителя направления мониторинга цифровых угроз «Лаборатории Касперского» Анны Павловской «Stack Overflow, Habr и внутренние вики: цифровой след или цифровой шлейф». Онлайн-конференцию посмотрели более 150 зрителей.

Старший менеджер по корпоративному маркетингу региона META Кристин Макдональд была отмечена отраслевой наградой Senior Marketing Leader of the Year по версии премии Women in Technology Forum and Awards 2025. Эта награда стала признанием ее вклада в развитие технологического сектора и усиление роли женщин в нем.

Компания профинансировала и поддержала выпуск специального эпизода подкаста Africaines in Tech, записанного в феврале 2025 года и опубликованного в ноябре. В этом выпуске старший менеджер по связям с государственными органами «Лаборатории Касперского» Глэдис Ядом рассказала о видении Компании и шагах, которые она предпринимает для укрепления инклюзивности женщин в сфере кибербезопасности во франкоязычных странах Африки.

В сентябре 2025 года «Лаборатория Касперского» и компания GRAMAX, надежный партнер в области защиты критически важной информационной инфраструктуры, провели специальную сессию Resilience in Action: The Women Beyond The Firewalls. Она была посвящена поддержке и продвижению женщин в кибербезопасности, изучению текущего положения женщин в отрасли, достигнутого прогресса и сохраняющихся вызовов. Генеральный менеджер «Лаборатории Касперского» в Индии Джайдиип Сингх представил инициативу Women in Tech. Программа также включала тематические доклады и панельные дискуссии о роли женщин в технологическом секторе.

Планы на 2026 год

В 2026 году мы продолжим развивать текущие проекты и запускать новые программы, направленные на предоставление женщинам равных возможностей для развития карьеры в разных направлениях в ИТ и ИБ. Мы планируем и дальше участвовать в отраслевых конференциях и форумах, публиковать истории успеха наших коллег, расширять образовательные инициативы и усиливать программы наставничества и карьерного развития для женщин по всему миру.

Поддержка сотрудников с ограниченными возможностями здоровья

«Лаборатория Касперского» поддерживает соискателей и сотрудников с ограниченными возможностями здоровья и стремится создать доступную и инклюзивную рабочую среду. Для нас важен человек и его потенциал, а не ограничения.

При найме мы оцениваем исключительно профессиональные навыки, опыт и экспертность кандидатов. Для ряда вакансий в Компании доступен удаленный формат работы, а при необходимости рабочее место может быть адаптировано в соответствии с индивидуальной программой реабилитации.

Всем сотрудникам с инвалидностью предоставляются все льготы, предусмотренные российским законодательством: увеличенный ежегодный отпуск (для всех групп инвалидности) и сокращенный рабочий день (для определенной группы людей с инвалидностью).

Развитие сотрудников

Мы создаем необходимые условия для профессионального роста и развития наших сотрудников — как индивидуального, так и в командах, поддерживая тем самым и развитие всего бизнеса.

При этом «Лаборатория Касперского» постоянно совершенствует подход к обучению и увеличивает инвестиции в развитие сотрудников на всех этапах их карьеры. Так, в 2025 году расходы на обучение и развитие персонала выросли на 12,6% по сравнению с предыдущим годом, а среднее количество времени обучения на одного сотрудника увеличилось на 14% и достигло 12,9 часа.

СОКБ 31

197,1 млн рублей
общие расходы на обучение сотрудников в 2024–2025 годах

17 тысяч рублей
расходы на обучение в расчете на одного сотрудника в 2025 году

Среднее количество часов обучения на одного сотрудника[1], часов

GRI 404-1, СОКБ 32

Категория сотрудников	2023	2024	2025
Среднее количество часов обучения всех сотрудников, в том числе:	9,2	12,1	11,4
■ руководителей	11,4	10,2	9,9
■ технических специалистов[2]	7,8	9,8	9,6
■ прочих специалистов	11,4	14	13

Нашим сотрудникам доступны возможности как внутреннего, так и внешнего обучения. В Компании можно пройти онлайн-курсы по продуктам и технологиям, программы по развитию бизнес-навыков, продаж и персональных компетенций, выбрать удобный формат изучения иностранных языков, найти ментора по профессиональным вопросам или подать заявку на участие во внешних тренингах и мероприятиях.

Обучение строится гибко: наряду с обязательными у нас реализуются дополнительные корпоративные образовательные программы по выбору сотрудников.

Отдельное внимание в «Лаборатории Касперского» уделяется развитию руководителей. В 2025 году мы пересмотрели подход к их обучению и объединили программы в единую систему Leadership Programs. Она включает два уровня:

- Start — для начинающих руководителей, тимлидов и сотрудников, готовящихся к роли руководителей. Данную программу мы полностью пересмотрели с точки зрения содержательной части и перезапустили уже как часть экосистемы обучения.
- Pro — для более опытных руководителей среднего звена, в командах которых уже есть тимлиды. Это новая программа — пилотный поток был запущен в 2025 году.

Обучение построено на практических кейсах и современных управленческих фреймворках и направлено на создание единой системы развития руководителей, развитие преемственности внутри Компании, выравнивание и усиление управленческой экспертизы, а также повышение мотивации и усиление культуры лидерства и стратегического партнерства.

63 тимлида
и **17 руководителей**
среднего звена участвовали в Leadership Programs в 2025 году

Дополнительно мы развиваем культуру обмена опытом внутри Компании. С этой целью в 2024 году «Лаборатория Касперского» запустила Grow Lab — программу внутреннего менторинга, которая помогает сотрудникам находить наставников и внутренних экспертов для развития прикладных навыков и решения сложных профессиональных задач. С момента запуска в программе приняли участие 94 пары «наставник — подопечный», а в 2026 году мы планируем расширить масштабы проекта.

[1] Данные в таблице указаны без учета данных МООС-платформ (онлайн-платформ с массовыми открытыми онлайн-курсами).
[2] Специалисты IT + все сотрудники R&D.

Обязательные курсы

GRI 404-2

В обязательную программу обучения для работников Компании входят следующие курсы.

Информационная безопасность

Какие бы меры безопасности мы ни внедряли, в конечном счете главный участник системы — это человек. Человеческий фактор является самым уязвимым аспектом с точки зрения информационной безопасности. Обучение основам кибербезопасности проходят все сотрудники «Лаборатории Касперского», даже если они напрямую не связаны с разработкой или продвижением наших решений. Из серии курсов по информационной безопасности наши сотрудники узнают о правилах работы с конфиденциальной информацией, учатся безопасно хранить пароли и данные аккаунтов, а также выявлять фишинговые письма и сайты.

Правила поведения при возникновении чрезвычайной ситуации

Возгорание, задымление, искрение электропроводки и аппаратуры, аварии и другие происшествия приводят к серьезному материальному ущербу и, что более важно, наносят вред здоровью и уносят жизни людей. Изучение правил безопасности обязательно для всех сотрудников «Лаборатории Касперского» и проводится для подготовки сотрудников к адекватным и слаженным действиям во время потенциальной чрезвычайной ситуации.

Антикоррупционное поведение

Сотрудникам любой современной компании необходимо понимать и соблюдать антикоррупционное законодательство. Следуя изученным в курсе правилам, наши сотрудники могут поддержать репутацию и целостность «Лаборатории Касперского», а также избежать возможных штрафов для Компании и личной ответственности.

Дополнительные обучающие программы и инструменты развития экспертизы

Помимо обязательных образовательных программ, сотрудники могут самостоятельно выбирать дополнительные форматы обучения для развития профессиональной экспертизы. Для этого в «Лаборатории Касперского» доступны дистанционные курсы на внутренней образовательной платформе, а также очные тренерские программы, направленные на развитие гибких навыков, управленческих и прикладных профессиональных компетенций.

Наши сотрудники имеют возможность:

- проходить обучение на внешних онлайн-платформах, таких как Udemy, LinkedIn Learning, Pluralsight и CBT;
- заниматься на очных тренингах и вебинарах на внутреннем портале обучения «Эквио»;
- участвовать в менторской программе GrowLab;
- участвовать во внешних профессиональных конференциях;
- при необходимости — обучаться у внешних провайдеров для поддержания и развития профессиональной экспертизы (в рамках бюджета подразделений);
- изучать иностранные языки в удобном формате, с учетом индивидуальных целей и рабочих задач.

В 2025 году мы обновили тренинги по коммуникациям, ключевыми преимуществами которых стали максимально близкие к бизнесу благодаря вовлечению экспертов кейсы.

Планы на 2026 год

В ближайших планах Компании — крупный перезапуск менторской программы GrowLab, расширение каталога онлайн-курсов Kaspersky Academy, включая тренинги на иностранных языках, а также формирование образовательных траекторий для комплексного развития — как по отдельным темам (например, channel-продажи или навыки коммуникации), так и в привязке к ролям и должностям.

Оценка эффективности персонала и вознаграждение

В «Лаборатории Касперского» выстроена целостная и прозрачная экосистема управления эффективностью и развитием талантов. Она направлена на достижение стратегических целей Компании за счет раскрытия потенциала каждого сотрудника. Эта экосистема состоит из трех взаимосвязанных элементов: регулярной оценки эффективности, прозрачности вознаграждения и карьерной мобильности.

Процесс оценки результативности сотрудников проходит по годовому циклу и включает несколько этапов:
- постановку годовых целей;
- самооценку сотрудника по итогам года;
- финальную оценку со стороны непосредственного руководителя.

В течение года ведется постоянное отслеживание прогресса, что позволяет своевременно корректировать цели и подходы к их достижению.

GRI 404-3

Мы постоянно оцениваем качество работы персонала Компании. В 2025 году регулярную оценку результатов и перспектив развития карьеры проходили 90% сотрудников (в 2024 году их доля составила 88%).

Ежегодный пересмотр вознаграждения сотрудников основан на результатах годового цикла оценки их эффективности. При этом учитываются следующие критерии:
- индивидуальная результативность сотрудника;
- текущий уровень дохода по отношению к рынку;
- ситуация на рынке труда;
- результаты и планы Компании.

Развитие персонала

Один из ключевых компенсационных принципов Компании — «Вознаграждение за результаты». Итоги оценки эффективности влияют на пересмотр вознаграждения и карьерную мобильность сотрудников.

После достижения определенного стажа в «Лаборатории Касперского» (от шести месяцев до одного года) всем сотрудникам становится доступно участие в программе внутренней мобильности. Программа обеспечивает поддержку на каждом этапе развития и открывает дополнительные возможности для профессионального роста, позволяя сотрудникам развиваться в команде единомышленников.

Производительность труда

СОКБ 62

Процесс оценки производительности труда представляет собой комплексную систему, направленную одновременно на развитие сотрудников и достижение бизнес-целей. В нее входят:
- постановка и оценка целей (performance review);
- регулярный сбор обратной связи сотрудников (встречи в формате «один на один», опросы формата 360, самооценка и другие инструменты);
- оценка компетенций и формирование индивидуальных планов развития.

Результаты оценки производительности влияют в том числе на карьерный рост сотрудников, их материальное вознаграждение, а также на объемы инвестиций в обучение и развитие.

Мы на постоянной основе отслеживаем свыше 800 различных HR- и бизнес-метрик, используя их для принятия управленческих решений. Наша цель как HR-функции — повышение показателя возврата инвестиций в персонал. Этот стратегический показатель помогает оценивать эффективность вложений в людей, принимать более взвешенные кадровые решения и находить ответы на сложные управленческие вопросы.

Вовлеченность сотрудников

Каждый год мы оцениваем уровень удовлетворенности сотрудников в рамках анонимного опроса YourVoice. Опрос помогает узнать их отношение к изменениям в Компании, корректировке стратегии, оценить уровень влияния на них различных драйверов, таких как оплата, социальный пакет, баланс работы и личной жизни, перспективы профессионального роста, атмосфера в команде и других.

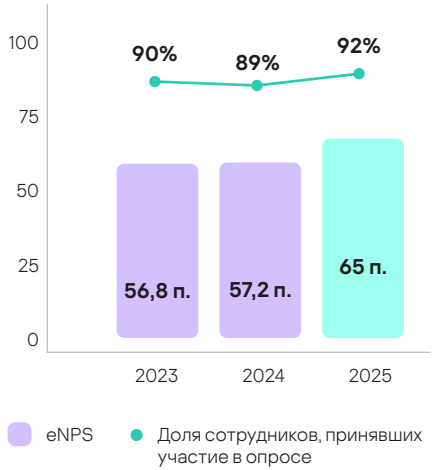
Ключевой показатель, на который мы ориентируемся, — это глобальный индекс удовлетворенности работой (eNPS), который отражает долю сотрудников, готовых рекомендовать Компанию как работодателя.

В 2024 году eNPS вырос по сравнению с предыдущим годом на 0,4 п. п., до 57,2, а в 2025 году — на 8 п. п., до рекордных 65.

Результаты опроса доступны руководителям всех уровней — это помогает анализировать ситуацию по командам, регионам, дивизионам и определять точки роста.

SASB TC-SI-330a.2

Индекс удовлетворенности сотрудников Компании



Мы регулярно информируем коллег о новостях, планах и изменениях в Компании, вовлекаем их в корпоративные инициативы через цифровые и офлайн-инструменты:
- статьи и публикации на внутреннем портале;
- публикации в закрытом канале в социальной сети;
- email-рассылки.

Также мы проводим сессии с топ-менеджерами Компании и представителями различных функций в формате AMA (Ask Me Anything) — делимся результатами работы, обсуждаем планы, отвечаем на вопросы сотрудников в прямом эфире.

Здоровье и безопасность труда

Мы стремимся к тому, чтобы каждое рабочее место в «Лаборатории Касперского» было комфортным и безопасным, а у сотрудников был доступ к качественной медицинской помощи и поддержке.

Ключевые документы

GRI 403-1

- Трудовой кодекс Российской Федерации
- Положение по идентификации опасностей и определению уровня профессиональных рисков
- Инструкция о мерах пожарной безопасности
- Правила внутреннего трудового распорядка
- Положение о пропускном и внутриобъектовом режиме
- Обязательный интерактивный обучающий курс по порядку действий при возникновении чрезвычайной ситуации в офисных помещениях «Лаборатории Касперского»
- Политика в области охраны труда

GRI 403-9

0 несчастных случаев,

связанных с реализацией профессиональных рисков в 2024 и 2025 годах

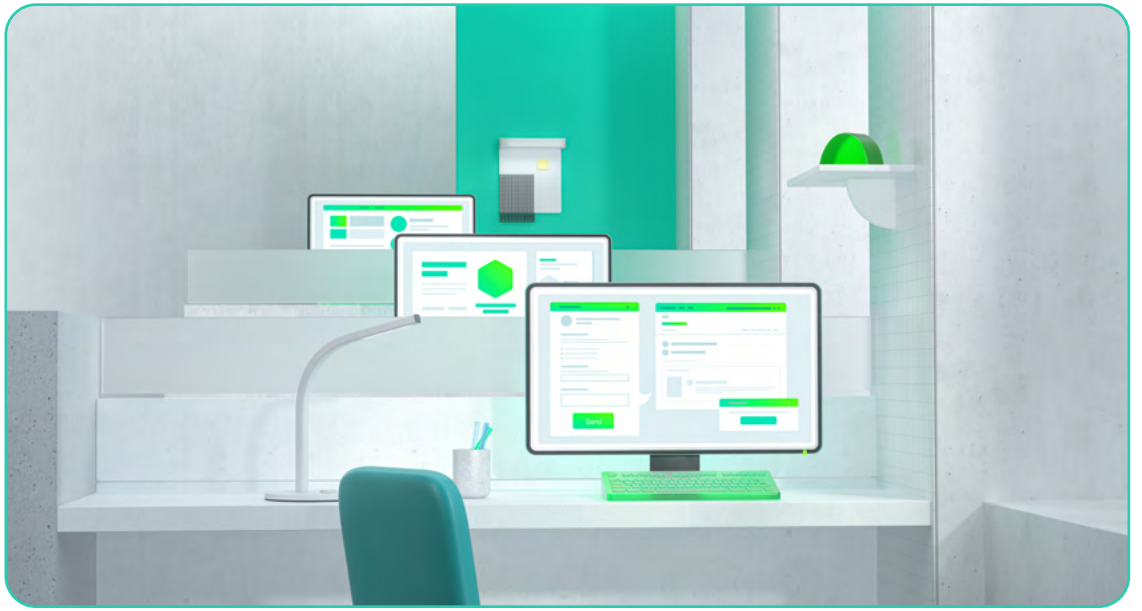
Управление охраной труда и здоровья

GRI 403-2, GRI 403-5

За безопасность труда в Компании отвечает департамент по работе с персоналом при поддержке внешних консультантов. В состав департамента входит группа кадрового администрирования, которая курирует вопросы охраны труда и здоровья сотрудников.

Система менеджмента охраны труда и здоровья во всех офисах «Лаборатории Касперского» в границах раскрытия в Отчете соответствует требованиям действующего трудового законодательства на территориях присутствия Компании. Она включает:

- регулярные инструктажи;
- регулярную специальную оценку рабочих мест во всех подразделениях;
- систему управления рисками и расследования несчастных случаев;
- организацию мероприятий по улучшению условий труда.



В рамках обучения и подготовки персонала в области охраны и безопасности труда сотрудники «Лаборатории Касперского» проходят вводный инструктаж при приеме на работу.

В настоящее время в Компании действуют следующие программы в области охраны и безопасности труда:

- программы вводных инструктажей по охране труда и по пожарной безопасности;
- программа обучения по общим вопросам охраны труда и функционирования системы управления охраной труда;
- программа обучения по противодействию чрезвычайным ситуациям.

Помимо этого, руководители Компании проходят обучение в учебном центре.

Ключевой показатель эффективности системы — отсутствие травм на рабочем месте.

GRI 403-9, СОКБ 29

Большинство сотрудников работают в офисе.
За отчетный период не было зафиксировано ни одного случая производственного травматизма или профессиональных заболеваний.

Работа в выходные и праздничные дни

Привлечение сотрудников к работе в выходные или нерабочие праздничные дни возможно по согласованию с департаментом по работе с персоналом и руководителем топ-департамента. Оно оформляется письменным согласием сотрудника, а факт выполненной работы отражается в табеле учета рабочего времени.

К работе в такие дни запрещено привлекать сотрудников, находящихся в отпуске, на больничном, а также беременных женщин. Продолжительность работы в выходной день не должна превышать восьми часов в неделю, а при работе в два выходных подряд — четыре часа в день.

Сотруднику, которого привлекают к работе в выходной или нерабочий праздничный день, предоставляются на выбор два вида компенсации:

- повышенная оплата;
- дополнительное время отдыха.

Как мы заботимся о здоровье и благополучии сотрудников

GRI 403-6

Сотрудники «Лаборатории Касперского» в России и их дети до 16 лет включительно охвачены корпоративной программой ДМС. В рамках программы для сотрудников также предусмотрено страхование от несчастных случаев. В случае происшествия информацию можно передать в страховую компанию через департамент по работе с персоналом.

Программа ДМС включает лечение онкологических заболеваний, стационарную помощь, психологическую поддержку онлайн и офлайн, ежегодные медосмотры для получения санаторно-курортной карты и вакцинацию от сезонных заболеваний.

В штаб-квартире Компании работают спортивный зал и сауна, доступны приемы терапевта, психолога и массажиста прямо в офисе. Также для наших сотрудников работает линия психологической помощи онлайн. Мы компенсируем часть расходов на оздоровление, включая оплату фитнеса и детских оздоровительных лагерей. Кроме того, сотрудники получают корпоративную скидку в сети аптек «Ригла».

GRI 403-4

Сотрудники могут оставить обратную связь после прохождения обязательного обучающего курса по противодействию чрезвычайным ситуациям. Также в рамках ежегодного анонимного опроса удовлетворенности мы измеряем восприятие сотрудниками уровня их физического, эмоционального и социального благополучия.

GRI 403-2

Как работодатель мы обеспечиваем персоналу безопасность условий труда в соответствии с государственными нормативными требованиями охраны труда. За отчетный период в Компании не было зарегистрировано ни одного инцидента, связанного с нарушением безопасных условий труда.

Несмотря на это, в «Лаборатории Касперского» предусмотрены доступные варианты реагирования на случай потенциального инцидента. В частности, сотрудники могут:

- обратиться на горячую линию поддержки сотрудников (HR Support);
- оставить заявку на внутреннем портале для команды административно-хозяйственного управления;
- записаться на прием к офисному врачу или психологу;
- обратиться напрямую к своему HR-бизнес-партнеру.

Вклад в развитие общества

71,3 млн рублей
расходы Компании на благотворительность в 2024–2025 годах

>200 университетов
в 45 странах сотрудничают с Kaspersky Academy

63% россиян
считают, что IT-компании должны адаптировать продукты для людей с инвалидностью

За пределами цифрового мира

GRI 203-1, GRI 203-2

Мы подходим к общественно полезной деятельности как к продолжению нашей основной миссии: стремление делать среду, в которой мы живем, безопаснее и устойчивее, для «Лаборатории Касперского» выходит за рамки цифрового мира.

71,3 млн рублей
прямые затраты на благотворительность за 2024–2025 годы

13,5 тысячи лицензий
безвозмездно передано благотворительным фондам

>16 млн рублей
экономия средств НКО за два года благодаря предоставлению Компанией бесплатных защитных лицензий

Общественно полезная деятельность для «Лаборатория Касперского» — это системная и долгосрочная работа, основанная на понимании реальных потребностей общества.

Мы стремимся поддерживать тех, кто особенно уязвим в цифровом и реальном мире, создавая инклюзивную и безопасную онлайн-среду. Мы хотим, чтобы люди чувствовали себя уверенно в интернете, понимали, как работают технологии, и умели ими пользоваться. Важное место в нашем подходе занимает и подготовка кадров для IT-отрасли — через развитие экспертизы, образовательные проекты и передачу знаний следующему поколению специалистов.

При этом наша помощь выходит за рамки прямой благотворительности — она создает положительное экономическое воздействие на местные сообщества и экономику. Значительная часть вклада «Лаборатории Касперского» в развитие общества проявляется через косвенный экономический эффект. Наши продукты и сервисы помогают компаниям, государственным организациям, НКО и частным пользователям снижать финансовые потери, вызванные киберинцидентами, повышать устойчивость цифровых процессов и укреплять доверие к онлайн-экономике.

Как мы помогаем фондам и НКО экономить средства

- **В отчетный период более 100 фондов** получили бесплатную киберзащиту от Компании
- **>16 млн рублей** — экономия средств НКО за два года благодаря выписанным Компанией бесплатным защитным лицензиям

«Лаборатория Касперского» регулярно помогает благотворительным фондам и НКО, обеспечивая надежную защиту их цифровой жизни от взломов, утечек и вирусов. Мы предоставляем бесплатные лицензии для стационарных ПК и ноутбуков, а также по необходимости для телефонов сотрудников и серверов этих организаций.

Например, ежегодная экономия фондов составляет:

- до **860 тысяч рублей** — для фонда помощи хосписам «Вера»
- до **637 тысяч рублей** — для фонда «Подари жизнь»
- до **270 тысяч рублей** — для фонда «Дети наши»
- до **196 тысяч рублей** — для РООИ «Перспектива»
- до **160 тысяч рублей** — для фонда поддержки слепоглухих «Со-единение»

Что в результате

Такая существенная экономия позволяет организациям, особенно небольшим НКО, больше времени и средств тратить на нужды своих подопечных и свою уставную деятельность.

Отдельное направление нашего воздействия связано с инвестициями в цифровую инфраструктуру, исследования, экспертизу и образовательные инициативы в сфере кибербезопасности. Эти инвестиции оказывают как текущий, так и долгосрочный положительный эффект на местные сообщества и экономику регионов присутствия. Появляются новые рабочие места с высокой добавленной стоимостью, растет число квалифицированных кадров для IT-отрасли. Параллельно развивается партнерская экосистема, поддерживается малый и средний бизнес в сфере IT- и ИБ-услуг.

Мы также учитываем и возможные минусы: рост требований к кибербезопасности может увеличить издержки для малого бизнеса и НКО. Но эти эффекты ограничены и управляемы благодаря нашим образовательным программам, консультациям, доступным сервисам и бесплатным продуктам для уязвимых групп. В целом все воздействия мы оцениваем как преимущественно положительные, соответствующие целям устойчивого развития и снижающие цифровое неравенство.

Социальные и благотворительные проекты

Наш подход к социальным инвестициям

Социальные и благотворительные программы «Лаборатории Касперского» помогают тем, кто особенно нуждается в поддержке, и укрепляют связь Компании с людьми и сообществами в разных регионах.

Цель благотворительной деятельности «Лаборатории Касперского» — способствовать реализации ее главной миссии: строить безопасный и устойчивый мир, где люди могут использовать технологии для улучшения жизни на планете.

Главные задачи социальных и благотворительных программ:

- выстраивание и развитие долгосрочных партнерств с благотворительными фондами, НКО и образовательными учреждениями;
- развитие корпоративного волонтерства, включая спортивные, донорские инициативы и инициативы pro bono;
- предоставление бесплатных защитных решений НКО и уязвимым группам населения;
- вовлечение сотрудников в благотворительные проекты и корпоративный фандрайзинг;
- поддержка инклюзивных проектов, включая трудоустройство и менторство для молодых специалистов с инвалидностью;
- развитие цифровой грамотности и безопасного использования технологий у уязвимых групп;
- поддержка социальных, экологических и инклюзивных активностей внутри Компании и за ее пределами.

Основные направления благотворительной деятельности

Компания больше 15 лет поддерживает социальные проекты. В России мы помогаем более чем десяти фондам и НКО, как федеральным, например «Подари жизнь», «Вера» и «Синдром любви», так и региональным, таким как Нижегородский женский кризисный центр и «Живи». Мы поддерживаем пациентов с тяжелыми заболеваниями, социально незащищенных граждан, жертв катастроф и пожилых людей.

Важную роль в этой деятельности играет корпоративный фандрайзинг — мы поддерживаем сборы партнеров-НКО и организуем собственные, приуроченные к важным датам и праздникам. В 2024 году в рамках внутренних фандрайзинговых мероприятий сотрудники «Лаборатории Касперского» собрали более 500 тысяч рублей, а в 2025 году — более 1 млн рублей Они были направлены фондам «Синдром любви», «Игра», «Подари жизнь», «Дом с маяком», «Подарок ангелу», «Ника», «Природа и люди» и «Второе дыхание».

>1,5 млн рублей

собрали сотрудники Компании для благотворительных фондов в 2024–2025 годах

Как мы поддерживаем фонды и НКО

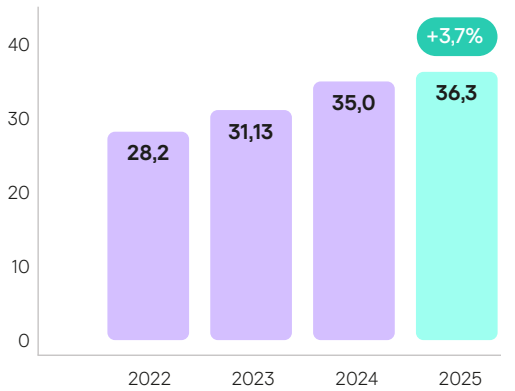
Одно из ключевых направлений нашей социальной работы — технологическая поддержка некоммерческого сектора. Компания участвует в федеральном проекте «Технологии добра», который помогает НКО получать доступ к цифровым продуктам и сервисам бесплатно или на льготных условиях. Проект реализуется ПАО «Совкомбанк» и Skolkovo Fintech Hub.

В отчетном периоде мы безвозмездно передали свыше 13 500 лицензий на защитные продукты более чем 100 благотворительным фондам и НКО. Бесплатные лицензии получили также свыше 200 частных лиц — люди с инвалидностью, многодетные семьи и люди, оказавшиеся в сложной жизненной ситуации.

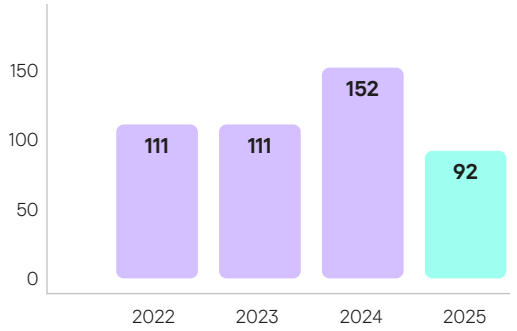
В 2024 году «Лаборатория Касперского» начала сотрудничать с Российским Красным Крестом, предоставив ему решения для защиты инфраструктуры и онлайн-ресурсов — Kaspersky Endpoint Detection and Response Optimum и Kaspersky DDoS Protection. После начала сотрудничества организация не сталкивалась с проблемами доступности сайта, несмотря на ранее зафиксированные кибератаки.

СОКБ 35

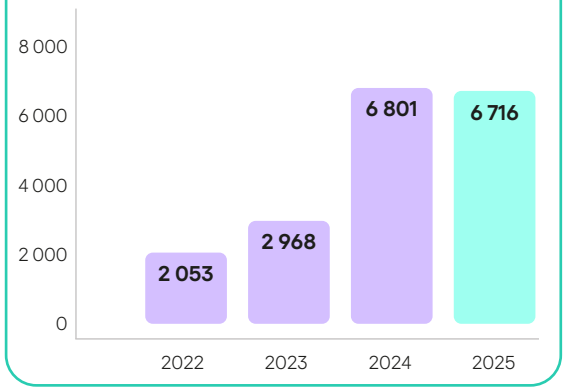
Расходы на благотворительность, млн рублей



Лицензии, переданные безвозмездно частным пользователям, нуждающимся в помощи, шт.



Лицензии на продукты, переданные безвозмездно благотворительным фондам, шт.



Как мы поддерживаем фонд «Игра»

Помогаем расширять базу знаний молодых специалистов в России и развивать современные подходы к терапии двигательных нарушений у детей

С 2022 года «Лаборатория Касперского» поддерживает фонд «Игра», который помогает детям с двигательными нарушениями жить более активной и самостоятельной жизнью. Речь идет не только об адресной помощи семьям, но и о развитии всей системы поддержки через обучение специалистов и доступ к современным знаниям.

В 2022 году фонд попросил у Компании помощи в приобретении международной терапевтической методики, которая помогает специалистам ставить цели лечения и оценивать его результаты. В России такие инструменты были доступны лишь точечно и чаще всего в виде неофициальных переводов.

При поддержке «Лаборатории Касперского» фонд перевел методические материалы на русский язык, получил образовательную лицензию и запустил обучающий курс для врачей и реабилитологов. Программа была посвящена клиент-центрированному подходу, SMART-целеполаганию в терапии и оценке изменений качества жизни детей по итогам лечения.

Что в результате?

- **~300** специалистов прошли обучение современным терапевтическим подходам к концу 2025 года.
- **45** реабилитационных организаций приняли участие в программе.
- **3** благотворительные службы для детей с двигательными нарушениями от рождения до трех лет внедрили шкалы оценки ранней помощи в регулярную работу.
- **2** специалиста начали годовую программу переквалификации, чтобы освоить профессию эрготерапевта — самую дефицитную в сфере помощи детям с инвалидностью.
- **33** региона России охвачены инициативой.

Для многих врачей это стало революционной возможностью по-новому взглянуть на свою работу и применять более бережные и современные методы помощи детям. А для семей — получать качественную терапию ближе к дому, не выезжая в крупные федеральные центры.

В 2025 году приобретенные права на методические материалы легли в основу IT-платформы для врачей и реабилитологов, которая выиграла в конкурсе IT-сообщества Global CIO. Платформа бесплатно работает для тех специалистов, кто учился и перешел на пациент-центрированные технологии в помощи.

Следующим шагом стало расширение профессионального диалога. В 2024 году Компания поддержала участие российских специалистов в конференции Европейской академии детской инвалидности (EACD), которая прошла в Бельгии. Это одна из крупнейших международных площадок, где встречаются врачи, реабилитологи, ученые, пациенты и их семьи со всего мира.

При поддержке «Лаборатории Касперского» в конференции приняли участие четыре российских специалиста и директор фонда. В результате фонд смог наладить прямые контакты с ведущими мировыми экспертами, в том числе с основателем лаборатории CanChild, которая уже много лет разрабатывает практические решения для помощи детям с особенностями развития.

Одним из важных результатов этого сотрудничества стало соглашение о переводе на русский язык инструментов и шкал CanChild, предназначенных как для врачей, так и для родителей.

В 2025 году Компания вновь поддержала возможность участия в конференции — на этот раз прибыло уже семь делегатов от России. Впервые за 37 лет проведения конференции были представлены три российские научные работы: по постановке целей в реабилитации детей после лечения опухолей головного мозга и телереабилитации детей в удаленных регионах.

Как мы работаем с местными сообществами

GRI 413-1

В отчетном периоде «Лаборатория Касперского» усилила прямое взаимодействие с местными сообществами. Основной фокус был направлен на развитие цифровой грамотности, повышение уровня кибербезопасности и снижение цифрового неравенства среди школьников и студентов, родителей и педагогов, сотрудников НКО и социальных учреждений.

Мы внедряли и поддерживали образовательные и просветительские инициативы по безопасному использованию цифровых технологий, а также инклюзивные проекты в партнерстве с профильными организациями. Важную роль в этом играет вовлечение сотрудников Компании в образовательные и социальные мероприятия.

Подробнее об этом читайте в разделах «Инклюзивность в киберпространстве» на с. 80 и «Цифровое просвещение» на с. 87

Как мы привлекаем к благотворительности сотрудников

Мы регулярно организовываем мероприятия и акции, которые позволяют нашим сотрудникам участвовать в благотворительности. В 2024–2025 годах в московском офисе традиционно прошли две новогодние благотворительные ярмарки в пользу фонда «Живи». По итогам ярмарки 2024 года сотрудники вместе с Компанией собрали более 2,8 млн рублей, а в 2025 году — более 3,4 млн рублей. Эти средства были переданы региональным детским онкогематологическим отделениям.

В 2024 году средства, собранные на ярмарке, помогли улучшить условия лечения детей в Тульской детской областной клинической больнице и РДКБ им. Е. П. Глинки в Грозном. Они были направлены на закупку высокотехнологичного медицинского оборудования, модернизацию палат и общих зон отделений, организацию досуговых пространств и мероприятий для детей в стационаре, а также на создание дополнительных мест для лечения.

>6,2 млн рублей

собрано на благотворительных ярмарках для фонда «Живи» в 2024–2025 годах

В декабре 2024 года «Лаборатория Касперского» совместно с фондом помощи хосписам «Вера» выпустили и реализовали первую благотворительную коллекцию мерча, включая худи, футболки и шоперы. Половина выручки (более 500 тысяч рублей) была направлена на нужды фонда.

Вместе с фондом «Ника» мы также выпустили специальную коллекцию носочков для продажи на корпоративном Дне детей. Вся выручка от реализации (более 60 тысяч рублей) пошла на поддержку подопечных фонда. В будущем мы планируем выпустить и другие коллекции совместно с фондами-партнерами.

В июле 2025 года Компания поддержала мероприятие «Щедрый книжный», организованное Нижегородским женским кризисным центром. Мы помогли закрыть часть организационных расходов, привлекли сотрудников к волонтерству, предоставили книги для продажи и призы для лотереи. По итогам мероприятия центру удалось собрать более 750 тысяч рублей.

Наши волонтерские программы

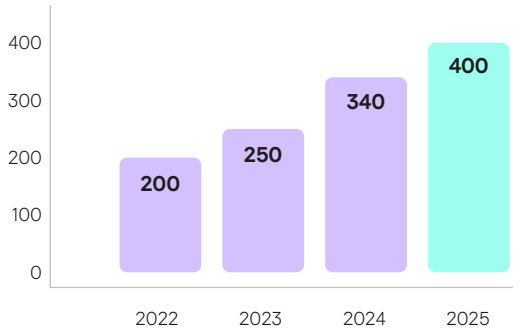
Корпоративное волонтерство в «Лаборатории Касперского» активно развивается каждый год. В 2024 году в волонтерских программах участвовали 340 сотрудников, а в 2025 году — уже около 400, то есть вдвое больше по сравнению с 2022 годом.

~400

сотрудников-волонтеров в 2025 году

СОКБ 37

Число сотрудников, участвующих в волонтерских программах Компании



В 2024 году «Лаборатория Касперского» вошла в Национальный совет по корпоративному волонтерству.

В 2024 году программы Компании включали несколько направлений: донорство крови, благотворительные спортивные мероприятия, патронаж детского дома, оказание бесплатной профессиональной помощи. За отчетный период в программу корпоративного волонтерства были добавлены новые инициативы в партнерстве с фондами «Дари еду», «Ника» и «Второе дыхание».

Донорство

Доноры — это крупнейшая команда волонтеров в Компании. Наши сотрудники дважды в год сдают кровь. Акция проводится в московском офисе «Лаборатории Касперского» совместно с Центром крови Федерального медико-биологического агентства (ФМБА) России.

В 2024 году кровь сдали 212 сотрудников, а в 2025 году — 215, причем около трети из них делали это дважды в год. В 2024 году на Всероссийском конкурсе «Корпоративная культура донорства» «Лаборатория Касперского» была отмечена Российским Красным Крестом в номинации «Лучший корпоративный день волонтера». Кроме сдачи крови, у сотрудников есть возможность пройти типирование для вступления в регистр доноров костного мозга.

Спортивное волонтерство

Спортивные волонтеры — это вторая по численности группа, которая сегодня объединяет 139 сотрудников (рост на 26,4% к 2024 году). В отчетном периоде «Лаборатория Касперского» стала спонсором 12 благотворительных спортивных мероприятий в пользу фондов «Синдром любви», «Вера», «Лейкозу нет» и «Бумажная птица». Наши волонтеры участвовали в забегах, сайклинг-марафонах, онлайн-триатлонах.

Мы продолжаем развивать этот формат, потому что он одинаково важен и для сотрудников, и для фондов-партнеров. Благотворительные спортивные мероприятия вовлекают большое количество единомышленников, и за несколько лет они сформировали в Компании активное сообщество любителей спорта. Для благотворительных фондов это один из способов говорить об инклюзии и привлекать внимание к социальным активностям, что очень важно и для Компании. А для сотрудников это возможность поддержать добрые дела и почувствовать командное единство, общаясь с коллегами из разных подразделений.

Субботники

Еще одно важное направление волонтерской работы — субботники и помощь хосписам, которые находятся под патронажем фонда «Вера». Это третья по численности волонтерская группа компании: за 2024–2025 годы число волонтеров, участвовавших в ней, увеличилось в 1,5 раза, и это позволило нам браться за более масштабные задачи.

Два раза в год волонтеры приезжают в московские хосписы и центры паллиативной помощи, чтобы помочь с генеральной уборкой и благоустройством территорий. Они приводят в порядок помещения хосписа, убирают прилегающие пространства, высаживают цветы и берут на себя хозяйственные задачи — от закупки продуктов и воды до приобретения необходимых расходных материалов.

Благодаря субботникам удалось подготовить уличные пространства Первого московского детского хосписа к празднованию Дня детей и летнему сезону, а осенью — благоустроить территорию хосписа в Ростокино к его 22-летию.

Помимо хозяйственной помощи, наши сотрудники участвуют в сборе подарков для пациенток и сотрудниц хосписов. Так, в 2024–2025 годах к 8 Марта совместно с фондом «Вера» было собрано более 500 подарков.

Волонтерство pro bono

С 2022 года «Лаборатория Касперского» развивает направление волонтерства pro bono — оказание безвозмездной профессиональной помощи благотворительным фондам и некоммерческим организациям. Этот формат позволяет сотрудникам делиться своей профессиональной экспертизой и поддерживать партнеров в решении практических задач, повышая устойчивость НКО и расширяя возможности их работы.

В 2024–2025 годах специалисты Компании из разных подразделений участвовали в следующих проектах:

- **Стратегическая поддержка фонда «Синдром любви»**: команда российского маркетинга провела воркшоп, в рамках которого проанализировала кампании по продвижению фонда, используемые инструменты и каналы, метрики и КПЭ, а также предложила практические рекомендации для дальнейшего развития коммуникаций.
- **Менторство для студентов с инвалидностью**: сотрудники Компании выступили наставниками в программе «Попробуй профессию в деле», реализуемой РООИ «Перспектива», помогая участникам программы определиться с профессиональными интересами и сделать первые шаги в карьере.
- **Дизайн-поддержка «СПИД.Центра»**: отдел дизайна помог оформить интерактивную карту с базой верифицированных ВИЧ-сервисных организаций. Наши сотрудники превратили важные, но сложные данные в удобный цифровой инструмент для поиска ближайших центров помощи и доступных услуг.
- **Обучение кибергигиене для НКО**: наши эксперты по информационной безопасности провели тренинги по базовой кибергигиене и лекции о современных цифровых угрозах для сотрудников НКО, включая фонды «Перспектива», «Дети наши» и «Вверх».
- **Профориентационные мероприятия для подростков**: аналитик по кибербезопасности выступил спикером на мероприятии фонда «Детские деревни SOS», рассказав его подопечным о карьерных возможностях в сфере кибербезопасности.
- **Образовательные программы**: ведущие специалисты «Лаборатории Каперского» приняли участие в программе «Оставь свой след» компании «Деловые решения и технологии» (ДРТ). Они поделились знаниями о безопасной работе с ИИ, защите персональных и корпоративных данных и распознавании распространенных схем кибермошенничества.
- **Конференция «Технологии Добра»**: ведущий эксперт по исследованиям угроз информационной безопасности Компании модерировал сессию «От кибератак до социальной инженерии — как НКО и бизнесу эффективно защищать себя и свою аудиторию». Он поделился со слушателями реальной статистикой, примерами кибератак и рассказал об эффективных инструментах защиты.

Патронаж детских учреждений

Сотрудники «Лаборатории Касперского» продолжают поддерживать Удомельский детский дом и Тверскую школу № 4 — специализированный интернат для детей с задержкой психического развития, расстройствами аутистического спектра и нарушениями в работе опорно-двигательного аппарата. Мы на постоянной основе помогаем этим учреждениям как волонтеры, а также берем на себя часть организационных и бытовых забот.

Сотрудники Компании четыре раза в год приезжают в Удомельский детский дом и каждый раз тщательно готовят программу для воспитанников. В нее входят образовательные лекции, спортивные и творческие активности, игры и мастер-классы. Один раз в год волонтеры также организуют для детей летний поход с палатками — с костром, песнями и совместным отдыхом. Сотрудничество с Удомельским детским домом продолжается уже более 15 лет.

Перед каждой поездкой сотрудники помогают с закупкой всего необходимого для повседневной жизни и обучения воспитанников. Помимо этого, Компания участвует в проведении ремонтов, закупке оборудования и бытовых товаров, а также помогает с организацией поездок на отдых для воспитанников.

Новые активности

В 2025 году мы расширили программу корпоративного волонтерства, протестировав новые форматы сотрудничества с фондами-партнерами. Эти активности позволили сотрудникам «Лаборатории Касперского» включаться в помощь разным целевым группам: подросткам, пожилым людям и даже бездомным животным.

- **Поддержка выпускников в сложной жизненной ситуации**: в преддверии окончания учебного года сотрудники Компании стали волонтерами и координаторами на мероприятии фонда «Второе дыхание» — дне поддержки для выпускников в сложной жизненной ситуации. В этот день им помогают сформировать подходящий образ для праздничного вечера.
- **Помощь пожилым и маломобильным людям**: наши сотрудники выступили курьерами в проекте «Дари еду», помогая доставлять горячие обеды пожилым и маломобильным людям.
- **Волонтерство в приюте для животных**: состоялся первый визит сотрудников Компании в приют «Мокрый нос» фонда «Ника», где волонтеры выгуливали собак и общались с кошками. Такие визиты помогают животным социализироваться и повышают их шансы найти новый дом.
- **Участие в фестивале Woof**: мы присоединились к большой команде волонтеров фестиваля Woof, организованного фондом «Ника» в поддержку бездомных животных. Коллеги помогали в работе благотворительного маркета, вели социальные сети и фотосъемку, оформляли договоры, сопровождали гостей и участников фестиваля, а также участвовали в сборе и вручении подарков.

В 2026–2027 годах мы планируем развивать текущие инициативы и рассматриваем возможность запуска одного-двух совместных образовательных проектов с фондами-партнерами.

PetKa — решение для поиска пропавших питомцев в городах

Объединяем современные технологии, нашу экспертизу в области разработки приложений и возможность для людей помогать друг другу, чтобы вернуть питомцев домой.

Почему это важно
Потеря питомца — всегда тяжелое переживание. А поиск через объявления в соцсетях или группах часто занимает много времени и не дает результата.

41% россиян как минимум единожды теряли своего питомца[1]

Что сделано
Чтобы помочь хозяевам скорее отыскать питомца, «Лаборатория Касперского» запустила бесплатный цифровой сервис PetKa. Он дает возможность быстро распространять информацию о пропавших животных, а также объединять владельцев, волонтеров и всех, кто готов помочь.

Решение состоит из Kaspersky Tag — физической Bluetooth-метки, которую нужно закрепить на ошейнике животного, и PetKa — бесплатного приложения, которое позволяет отслеживать передвижения питомца при помощи Kaspersky Tag.

Пользователи PetKa также могут стать участниками «Команды Героев», созданной Компанией, получать сообщения о питомцах, потерявшихся поблизости, и помогать другим владельцам находить своих любимцев.

Результат
Поиск домашних животных стал проще и быстрее. Появилось удобное пространство, где люди помогают друг другу.

[1] По результатам исследования, проведенного «Лабораторией Касперского» среди 2 450 жителей крупных городов России, у которых есть домашние животные.

Инклюзивность в киберпространстве

Мы стремимся создавать среду, в которой люди с инвалидностью могут безопасно пользоваться цифровыми сервисами, развивать навыки и строить карьеру в IT.

Для «Лаборатории Касперского» инклюзивность в киберпространстве — это прежде всего равный доступ к знаниям, технологиям и возможностям профессионального развития.

Одно из ключевых направлений нашей работы — инклюзивное трудоустройство. С 2022 года Компания входит в Совет бизнеса по вопросам инвалидности, организованный РООИ «Перспектива», и участвует в совместных проектах, направленных на расширение возможностей для студентов и молодых специалистов с инвалидностью.

Наши сотрудники регулярно участвуют в ярмарках вакансий и профориентационных мероприятиях, включая конкурс «Путь к карьере» и ярмарки вакансий для студентов и молодых специалистов с инвалидностью, а также проводят экскурсии, профориентационные лекции и встречи в московском офисе. В 2025 году мы помогли организовать бизнес-завтрак, в котором участвовали более 30 представителей компаний, поддерживающих инклюзию.

Развиваем инклюзивные стажировки

В отчетном периоде мы продолжали развивать инклюзивное трудоустройство. «Лаборатория Касперского» приглашала студентов и недавних выпускников с инвалидностью к участию в программах стажировок в различных департаментах Компании.

В 2025 году мы провели исследование «ESG-практики в российских компаниях», которое показало: большинство россиян (63%) положительно отнеслись бы к тому, что к ним на работу взяли стажера с инвалидностью. Около трети респондентов восприняли бы это нейтрально.

Что в результате?

К концу отчетного периода все вакансии для стажеров с инвалидностью в Компании были закрыты. В 2026 году планируется масштабирование инклюзивных стажировок и открытие новых вакансий.

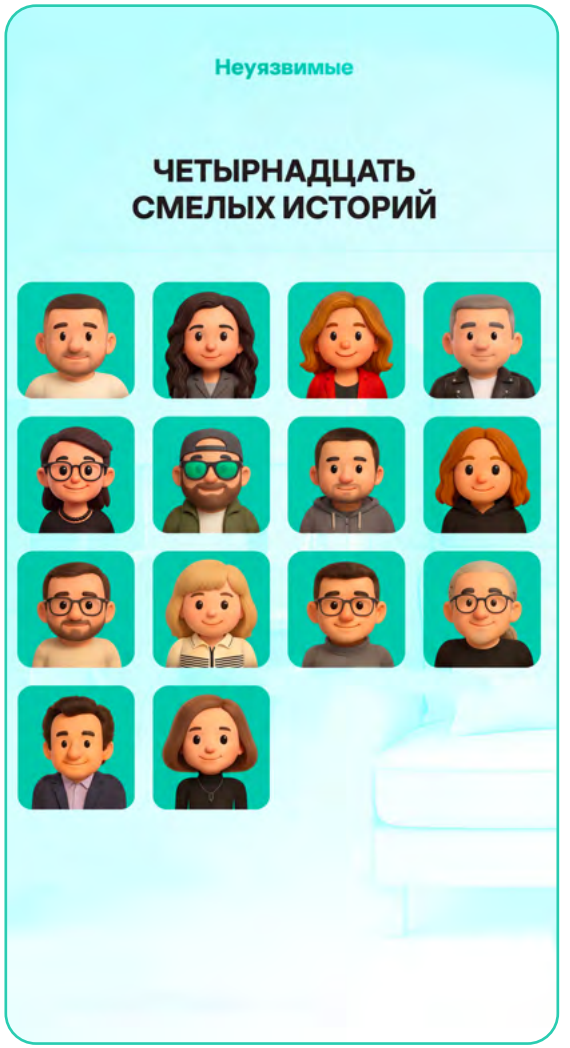
Мы также уделяем внимание физической и цифровой доступности рабочих пространств. Осенью 2024 года РООИ «Перспектива» провела аудит московского офиса Компании на предмет доступной универсальной среды и доступа к рабочим местам людей с инвалидностью и маломобильных граждан. По итогам аудита был подготовлен подробный отчет с рекомендациями, которые используются для дальнейшего улучшения офисных пространств.

Важной частью нашей работы остается формирование культуры принятия и снижение стигматизации. С 2022 года наша команда проектов устойчивого развития выпускает спецпроекты ко Дню людей с инвалидностью, рассказывая о профессиональном и личном опыте сотрудников с инвалидностью и родителей детей с инвалидностью.

В 2023 году был запущен сайт «Неуязвимые» с историями таких людей. Он ежегодно обновляется и пополняется новыми рассказами. В 2025 году проект получил новое развитие: теперь посетители сайта могут пройтись по виртуальному офису Компании, познакомиться с 3D-героями, получить справочную информацию о разных видах инвалидности и заболеваниях, а также поддержать программы инклюзивного трудоустройства РООИ «Перспектива».

Отдельное направление — цифровая грамотность для людей с ментальными особенностями. Осенью 2024 года совместно с фондом «Синдром любви» Компания представила первое в России методическое пособие по цифровой грамотности для людей с синдромом Дауна. В 2025 году проект начал масштабироваться: мы запустили сотрудничество с фондом «Кун бала» в Казахстане, передали технику для компьютерного класса и обучающие материалы. В дальнейшем мы планируем расширять географию проекта на другие регионы присутствия «Лаборатории Касперского».

Кроме того, в 2024 году Компания вновь присоединилась к всероссийской акции «Доброшрифт», приуроченной ко Дню поддержки людей с церебральным параличом, поддержав инициативу по повышению осведомленности об инклюзии и доступной среде.



Доступность цифровых ресурсов для людей с инвалидностью

Последние несколько лет Компания системно повышает доступность корпоративных цифровых ресурсов. Ключевые корпоративные сайты, включая пользовательские (B2C) страницы, корзину и сервисы поддержки, были адаптированы с учетом требований доступности, а сами принципы доступности интегрированы в процесс разработки и обновления цифровых продуктов.

В отчетном периоде работа была сфокусирована на развитии устойчивых процессов: внедрены автоматические тесты доступности, а требования к продуктам закреплены в стандартах разработки, что позволяет учитывать их на этапе создания новых функциональностей. Благодаря компонентной архитектуре многие улучшения, реализованные для B2C-сегмента, масштабируются и на B2B-сайты.

Дополнительно «Лаборатория Касперского» проводит пользовательские исследования с участием людей с инвалидностью. В частности, были организованы тестирования с незрячим пользователем, который проходил сценарии покупки и обращения в службу поддержки. Результаты таких исследований используются для выявления барьеров и приоритизации доработок.

При этом на текущий момент не все корпоративные цифровые ресурсы полностью соответствуют требованиям доступности. В частности, отдельные небольшие подсайты, которые разрабатываются и поддерживаются ограниченными ресурсами, пока не прошли полноценную адаптацию. Компания осознает наличие таких ограничений и ищет возможности их поэтапного устранения, чтобы обеспечить единый уровень доступности для всех цифровых платформ.

Работа по повышению доступности носит непрерывный характер: мы регулярно совершенствуем интерфейсы (в том числе дорабатываем элементы навигации, такие как переключатели режимов отображения), а также развиваем внутренние процессы и методические материалы, направленные на поддержание и дальнейшее улучшение уровня доступности цифровых сервисов.

Подготовка кадров для IT-отрасли

GRI 3-3

Мы системно развиваем кадровый потенциал в IT и кибербезопасности: готовим специалистов заранее, соединяем обучение с практикой и поддерживаем профессиональный рост на всех этапах.

52%

компаний считают, что подвергаются риску, связанному с неосторожными действиями собственных сотрудников

46%

инцидентов в 2024 году стали возможны из-за неосведомленности персонала

Наш подход к обучению

Дефицит квалифицированных специалистов в IT и кибербезопасности — одна из ключевых проблем отрасли. По данным исследования «Лаборатории Касперского», опубликованного в 2024 году, за предыдущие два года большинство компаний хотя бы раз сталкивались с киберинцидентами, связанными с нехваткой профильных специалистов.

При этом 52% организаций считают, что находятся под угрозой изнутри: ошибки, неосторожные действия или недостаток знаний сотрудников напрямую влияют на уровень информационной безопасности бизнеса[1].

В 46% инцидентов за 2024 год именно неосведомленность или небрежность персонала стала фактором, способствовавшим атаке.

Мы исходим из того, что подготовка кадров — это непрерывный процесс. Чтобы специалисты были готовы к реальным вызовам, работать нужно системно, начиная со школьного возраста и заканчивая программами повышения квалификации для опытных профессионалов.

Именно поэтому «Лаборатория Касперского» развивает комплекс обучающих инициатив, охватывающих аудиторию от школьников до действующих IT- и ИБ-специалистов. Мы создаем онлайн-курсы, проводим хакатоны[2] и конкурсы, поддерживаем проведение олимпиад, организуем оплачиваемые стажировки. Также реализуем совместные обучающие проекты с университетами, государственными структурами и локальными профессиональными сообществами.

Kaspersky Academy и сотрудничество с вузами

Чтобы масштабировать обучающие проекты и сделать их доступными для всех желающих, в 2010 году Компания запустила Kaspersky Academy — глобальную образовательную платформу в области информационной безопасности.

За 2022–2025 годы в ней прошли обучение тысячи студентов из России, стран Европы, Ближнего Востока, Африки, а также Южной и Юго-Восточной Азии, Латинской Америки.

Сегодня Kaspersky Academy объединяет курсы, тренинги и практические форматы обучения для широкой аудитории — от школьников и студентов до специалистов и пользователей без технической подготовки. В качестве спикеров и авторов программ выступают руководители направлений и ведущие эксперты по кибербезопасности «Лаборатории Касперского».

В отчетном периоде Компания сосредоточилась на развитии доступных и практико-ориентированных учебных форматов, в том числе:

- в рамках Kaspersky Academy запущен бесплатный онлайн-курс «Кибергигиена», который помогает пользователям освоить принципы безопасного использования гаджетов и интернет-сервисов. Программа включает 16 видеоуроков продолжительностью 15–20 минут;
- запущен курс «Введение в кибербезопасность» как для IT-специалистов, так и для пользователей без технической подготовки;
- создан онлайн-курс для старшеклассников и студентов «Кто ты в ИТ», который помогает им разобраться в профессиях в сфере IT и информационной безопасности, а также определиться с направлением для карьерного развития. Программа состоит из 30 коротких видеоуроков до 25 минут и охватывает более 20 специальностей — как технических, так и гуманитарных.

Параллельно мы расширяем сотрудничество с университетами. Сегодня Компания взаимодействует более чем с 200 вузами в 45 странах мира, включая более 70 учебных заведений в России и странах СНГ. Мы организуем совместные хакатоны и соревнования, создаем лаборатории и разрабатываем совместные учебные программы, предоставляем доступ к технологиям и экспертизе Компании, а также предлагаем студентам стажировки и участие в прикладных проектах.

С нами сотрудничают:

>200

университетов в 45 странах

в том числе:

>70

вузов в России и странах СНГ

[1] По данным исследования, проведенного Kaspersky Lab и B2B International среди более чем 5 000 компаний по всему миру.

[2] Хакатон — событие, где IT-специалисты совместно разрабатывают решение поставленной задачи.

Kaspersky Academy Alliance

В 2023 году «Лаборатория Касперского» запустила специальную партнерскую программу Kaspersky Academy Alliance, которая позволяет университетам интегрировать наши курсы, технологии и практики в образовательный процесс. Программой Kaspersky Academy Alliance заинтересовались многие учебные заведения — к концу 2025 года было подписано 50 соглашений с вузами из 16 стран.

Помимо университетов, мы активно сотрудничаем с государственными и образовательными организациями, а также с локальными профессиональными сообществами в странах Ближнего Востока, Африки, Южной и Юго-Восточной Азии, Латинской Америки.

Так, в 2025 году были подписаны соглашения о сотрудничестве с Министерством цифровой экономики и предпринимательства Иордании (MoDEE) и Tuwaiq Academy (национальным образовательным центром Саудовской Аравии в сфере цифровых технологий и программирования).

~50 вузов

из разных стран присоединились к программе Academy Alliance за два года

Как мы развиваем практические навыки

Практика играет ключевую роль в подготовке специалистов по кибербезопасности, поэтому важное место в нашей образовательной экосистеме занимают соревнования, олимпиады и экспертные сообщества.

Международные соревнования для экспертов по кибербезопасности

Развиваем профессиональное сообщество через практическое обучение

Capture the Flag (CTF) — это общепринятый с 1993 года формат соревнований по информационной безопасности, где участники ищут «флаги» (специальные файлы или данные), спрятанные в уязвимых программах, веб-сайтах или аппаратных устройствах.

«Лаборатория Касперского» популяризирует этот формат через соревнование **SAS CFT**, которое состоит из двух этапов, отборочного онлайн-тура и очного финала, и Kaspersky{CTF} — онлайн-соревнования, победители которого также принимают участие в финале SAS CTF.

Заключительный этап проводится в рамках собственной международной конференции Компании Security Analyst Summit, которая объединяет лучших экспертов со всего мира.

Что в результате

CTF-соревнования позволяют участникам совершенствовать свои навыки и обмениваться опытом. А для Компании это способ развивать международное сообщество исследователей и помогать отрасли готовить специалистов, которые умеют действовать быстро, совместно и нестандартно.

2024

SAS CTF 2024

В отборочном онлайн-туре приняли участие свыше 840 команд более чем из 80 стран. На этом этапе проверялись навыки реверс-инжиниринга, анализа уязвимостей бинарных файлов, цифровой криминалистики, стеганографии и программирования;

В финале, который прошел в формате Attack-Defense, участвовали восемь команд, в том числе из России, Китая, Японии. Проверялись навыки участников: умение выявить уязвимости, исправить их для защиты сервисов от атак других команд, а также разработать эксплойты для атак на соперников в сети.

Победителем стала команда Bushwhackers (Россия), которая получила **$10 000** за первое место. Общий призовой фонд составил $18 000.

2025

24-часовой онлайн-турнир Kaspersky{CTF}

Чтобы дать возможность ИБ-специалистам и студентам со всего мира усилить свои компетенции, 30–31 августа, мы представили новое соревнование Kaspersky{CTF}, в котором приняли участие 1 100 академических и 490 корпоративных команд.

- **1 600 команд** из **90 стран** соревновались онлайн.
- Команды решали серию задач в области реверс-инжиниринга, криптографии, бинарной эксплуатации, веб-безопасности и цифровой криминалистики.
- Все **25 задач** были успешно решены.
- Были определены **5 победителей** из **5 регионов** (Ganesh (Бразилия), Pinely (Нидерланды), SolidAll (Россия), PwnSec (ОАЭ) и Odin (Южная Корея).
- Эти команды были приглашены на финал соревнования **SAS CTF** (Као-Лак, Таиланд).

Новые соревнования отражают стремление Компании способствовать развитию академического сообщества через практическое обучение.

SAS CTF 2025

В отборочном онлайн-туре приняли участие более 900 команд из более чем 80 стран. На этом этапе проверялись способности находить уязвимости, решать криптографические головоломки и задачи, связанные с искусственным интеллектом.

Всего в финал вышли 13 команд (из стран Европы, Ближнего Востока, Азиатско-Тихоокеанского региона и Латинской Америки): восемь через SAS CTF, и еще пять — через Kaspersky{CTF}. Участники одновременно защищали свою инфраструктуру и атаковали инфраструктуры других команд. Каждая команда получала доступ к одинаковым серверам, содержащим уязвимые сервисы. Им нужно было найти уязвимости, исправить их на своем сервере и эксплуатировать те же уязвимости на серверах конкурентов.

Команды боролись за призовой фонд в $18 000, а победителем стала команда **C4T BuT S4D** (Россия), которая получила $10 000 за первое место.

В июле 2025 года «Лаборатория Касперского» совместно с Технологическим институтом Манипала в Бангалоре (MIT Bengaluru) провели HackSky 2025. Это национальный паниндийский хакатон по кибербезопасности, собравший молодых разработчиков и студентов со всей Индии для решения реальных задач в области защиты данных и IT-безопасности.

Хакатон длился 48 часов: участники интенсивно трудились, разрабатывая инновационные решения на стыке технологий и безопасности. Победителями стали студенты команды MIT Tech Wizards из MIT Bengaluru, продемонстрировавшие лучшие навыки и практические результаты. Организаторы мероприятия обеспечили призовой фонд и возможности для дальнейшей поддержки проектов и карьерного развития молодых киберталантов в Индии.

На международном форуме Kazan Digital Week 2025, партнером которого выступила «Лаборатория Касперского», эксперты Компании делились прикладными кейсами внедрения кибериммунной архитектуры KasperskyOS, практикой применения ИИ для анализа телеметрии и выявления инцидентов. Специалисты также демонстрировали реальные сценарии защиты цифровой инфраструктуры транспорта и промышленности. Такой формат — разбор прикладных проектов, технологические демонстрации и профессиональные дискуссии — способствует развитию практических компетенций у участников, включая студентов профильных направлений.

Работаем с одаренными школьниками

Отдельное направление нашей работы — поддержка одаренных школьников. В 2024–2025 годах Компания участвовала в подготовке и проведении международных олимпиад по кибербезопасности. Старшеклассников готовили ведущие специалисты в области кибербезопасности из «Лаборатории Касперского» и Центрального университета.

Первая Международная олимпиада по кибербезопасности (International Cybersecurity Olympiad, ICO) прошла в июне 2025 года в Сингапуре. В состав российской команды вошли восемь учащихся 11-х классов из Москвы и Казани, которые встретилась с 128 талантливыми школьниками из 25 стран. В итоге участники из России завоевали восемь медалей, в том числе три золотых.

Такие олимпиады способствуют развитию практических навыков и профессионального интереса у будущих специалистов. Мы планируем продолжать эту работу и в 2026 году.

Экспертное сообщество Kaspersky Academy

Чтобы поддержать не только школьников и студентов, но и академическое сообщество, мы развиваем экспертное сообщество Kaspersky Academy. Это серия профессиональных мероприятий для преподавателей, исследователей, деканов и заведующих кафедрами в области информационной безопасности и смежных дисциплин.

Один раз в квартал мы проводим для них встречи, на которых специалисты Компании делятся своей экспертизой по актуальным темам. Также проходят регулярные бесплатные двух- или трехдневные тренинги для преподавательского состава вузов под руководством наших экспертов.

География экспертного сообщества Kaspersky Academy очень широкая, она охватывает практически всю Россию и страны СНГ. В отчетном периоде мы расширили проект и на другие страны.

- **Встречи в России**: за 2024–2025 годы мы провели семь мероприятий сообщества (в среднем по 30–35 участников), а также четыре двухдневных тренинга для преподавателей и специалистов вузов России и стран СНГ (в среднем около 35 участников).
- **Международные мероприятия**: в 2025 году прошли тренинги в Турции для преподавателей из 20 университетов, CyberDay в Иордании, который собрал представителей более чем 20 вузов, образовательные мероприятия для академического сообщества в Гонконге (шесть учебных заведений) и Малайзии (девять университетов). Эти форматы объединяют преподавателей и студентов, позволяют обсуждать современные вызовы кибербезопасности и внедрять практико-ориентированные подходы в образовательные программы.

Наши планы на 2026–2027 годы

- **Углубление сотрудничества с вузами в России.** Мы планируем расширять инвестиции в образовательные программы, развивать взаимодействие с университетами с учетом обновляющихся требований к подготовке IT-кадров, увеличивать число вузов-партнеров и запускать совместные проекты.
- **Расширение международного присутствия.** Продолжим развивать образовательные инициативы и партнерства в странах Ближнего Востока и Африки, Южной и Юго-Восточной Азии, а также Латинской Америки — как через сотрудничество с образовательными организациями, так и через работу с локальными профессиональными и студенческими сообществами.

Как мы растим IT-специалистов

Мы помогаем сотрудникам и студентам прокачивать свои навыки в кибербезопасности: обучаем работе с реальными угрозами, делимся опытом ведущих экспертов и поддерживаем уверенный старт карьеры в IT.

Развиваем портал Kaspersky Expert Training

Развитие технологий и изменения в законодательстве постоянно формируют новые требования к специалистам по кибербезопасности. Поэтому непрерывное обучение является неотъемлемой частью профессии. Чтобы помочь специалистам актуализировать знания и осваивать современные инструменты, мы развиваем практико-ориентированную систему обучения на платформе Kaspersky Expert Training.

Онлайн-курсы в формате самообучения для проекта разрабатывают ведущие эксперты «Лаборатории Касперского», которые ежедневно работают с сотнями тысяч образцов вредоносного ПО и реальными инцидентами. Теория в обучении всегда подкрепляется практикой: в виртуальных лабораториях обучающиеся выполняют задания и разбирают кейсы, основанные на актуальных угрозах и сценариях, с которыми специалисты сталкиваются в работе.

Программы курсов рассчитаны как на отдельных специалистов по кибербезопасности, так и на компании, которые хотят обучить свои ИБ-команды (SOC, SERT и др.). Наши курсы могут быть полезны исследовательским институтам, центрам реагирования на инциденты и правительственным организациям.

Навыки, которые можно развивать в Kaspersky Expert Training:

- безопасная разработка ПО;
- активный поиск и обнаружение угроз;
- реагирование на инциденты и цифровая криминалистика;
- создание защищенных программных продуктов.

Для обучения доступны как базовые курсы, рассчитанные на любой уровень подготовки, так и продвинутые — для экспертов и профессионалов с опытом. В числе инструментов, использованию которых мы обучаем для обеспечения защиты, — Ghidra, Yara, Suricata, Frida.

В 2024–2025 годах портал пополнился тремя новыми онлайн-курсами:

- **Windows Digital Forensics** — цифровая криминалистика в Windows. Курс позволяет освоить методы обнаружения различных цифровых улик и управления ими в рамках криминалистической экспертизы, а также попрактиковаться в применении специальных инструментов для сбора улик и анализа артефактов в Windows;
- **Безопасная разработка ПО.** Курс освещает лучшие практики безопасной разработки ПО и учит эффективно интегрировать их в процессы создания продуктов;
- **Large language models security** — безопасность LLM. Курс по основам безопасности больших языковых моделей (LLM) на примере реальных атак, стратегий защиты и систем безопасности.

>3 000
пользователей более чем из 50 стран — аудитория тренингов для экспертов

>200
сотрудников «Лаборатории Касперского» получили бесплатный доступ к курсам Kaspersky Expert Training в 2024–2025 годах

74,5 часа
в среднем проводили студенты за прохождением курса о продвинутых техниках анализа вредоносного ПО

13 онлайн-тренингов
включает портфель Kaspersky Expert Training

В дополнение к образовательным курсам был запущен новый онлайн-проект — «Карта профессий в ИБ», который раскрывает все многообразие ролей в сфере кибербезопасности. Проект показывает особенности каждой роли, необходимые компетенции и возможные карьерные траектории. Разобраться в ИБ-ролях и получить необходимые навыки пользователям помогают кибергерои, каждый из которых воплощает одно из ключевых направлений.

Проект интегрирован с платформой Kaspersky Expert Training и служит удобной отправной точкой для профессионального развития. После прохождения теста на профориентацию каждый участник может получить персонализированные рекомендации по обучению, включая подбор соответствующих онлайн-курсов или тренингов. Это позволяет пользователям выбрать верное направление и выстроить последовательный путь развития.

В 2025 году совместно с командой Центра сервисов по кибербезопасности мы также запустили новое направление обучения — экспертно-продуктовые тренинги для специалистов, работающих с решениями «Лаборатории Касперского», такими как KATA (Kaspersky AntiTargeted Attack), KUMA (Kaspersky Unified Monitoring and Analysis Platform) и EDR (Kaspersky Endpoint Detection and Response). Эти программы помогают глубже разобраться в возможностях продуктов и научиться эффективно использовать их для обнаружения угроз и автоматизации реагирования.

Отдельное внимание уделяется локализации обучения. В 2024 году платформа заработала в России и на русском языке стали доступны три тренинга: «Реагирование на инциденты в Windows», «Техники продвинутого анализа вредоносного ПО» и «Безопасная разработка ПО». В конце 2025 года появилась также локализованная версия программы «Использование Suricata для поиска угроз и реагирования на инциденты».

Самым трудоемким стал курс по продвинутым методам анализа вредоносного ПО — в среднем его прохождение занимало 74,5 часа. Наибольший интерес в 2025 году вызвали темы мониторинга ИБ и активного поиска угроз, а также реагирования на инциденты в Windows.

Кроме того, мы продолжаем проводить бесплатное обучение для международных правоохранительных организаций. В 2024 году тренинги прошли 32 сотрудника Интерпола, а в 2025 году стартовало обучение сотрудников Африпола, которое продолжится и в 2026 году.

В 2026–2027 годах мы планируем расширить портфель экспертных программ за счет тренингов по безопасности в машинном обучении и Threat Intelligence, а также частично обновить действующие курсы и продолжить их локализацию на русский язык.

Предлагаем программы стажировок

В «Лаборатории Касперского» действует оплачиваемая стажерская программа **SafeBoard**, которая помогает студентам погрузиться в работу и поработать бок о бок с экспертами отрасли.

Стажировки проходят два раза в год — весной и осенью. Отбор включает тестирование технических знаний и практические задания, а сам процесс выстроен так, чтобы путь кандидата был максимально прозрачным и комфортным. Студентам, проживающим в Москве и Московской области, нужно подать заявку и пройти онлайн-отбор, состоящий из записи видеоинтервью, тестирования и тестового задания. Кандидаты, успешно справившиеся с отборочными заданиями, могут получить предложение о работе по итогам прохождения интервью с нанимающими экспертными командами.

Чтобы сделать путь кандидата в Компанию максимально быстрым и комфортным, в 2025 году мы полностью перевели процесс отбора в нашу рекрутмент-систему и перешли на единый процесс отбора. Теперь кандидаты получают все задания сразу и скорость прохождения этапов во многом зависит от них самих.

Летом 2025 года мы отметили 10-летний юбилей программы SafeBoard. Масштабный праздник объединил почти 500 участников, в том числе присоединившихся к онлайн-трансляции, — студентов, стажеров и сотрудников, начавших карьеру в Компании со стажировки.

Мы постоянно анализируем обратную связь от стажеров и наставников, чтобы совершенствовать проект, и продолжаем инвестировать в адаптацию новичков. Все стажеры получают онбординг[1]-материалы и рекомендации по обучению, которые помогают им быстрее освоиться и начать продуктивно работать.

Итоги 10 лет действия программы SafeBoard

>800 стажеров
пришли в «Лабораторию Касперского»

>350 выпускников
продолжают работать в Компании

>200 выпускников
работают в Компании на позиции Middle и выше

[1] Онбординг — процедура знакомства нового сотрудника/стажера с компанией и его адаптации в команде.

Цифровое просвещение

GRI 3-3

«Лаборатория Касперского» развивает проекты по повышению цифровой грамотности общества через доступное обучение и практические проекты для разных аудиторий.

Как мы обучаем пользователей основам кибербезопасности

Мы убеждены: чтобы технологии приносили пользу, людям важно понимать, как они работают, какие риски существуют в онлайн-среде и как защитить себя и своих близких. Поэтому мы развиваем просветительские инициативы, которые простым и понятным языком объясняют основы кибербезопасности и формируют ответственное отношение к цифровым технологиям.

Одно из ключевых направлений нашей работы — обучение по правилам цифровой безопасности. Мы рассказываем, как распознавать телефонное и онлайн-мошенничество, защищать персональные данные, безопасно пользоваться подключенными устройствами и цифровыми сервисами. Такие знания помогают людям осознанно принимать решения в диджитал-среде и снижать риски в повседневной жизни.

Говорим о кибербезопасности просто и понятно

«Лаборатория Касперского» создала несколько просветительских проектов для людей любого уровня вовлеченности в кибербезопасность — от экспертов по ИБ до обычных пользователей интернета. Подкасты «Смени пароль!» и «ОБИБЭ» рассказывают о цифровых рисках, кибергигиене и современных угрозах. Они охватывают и универсальные темы, актуальные для каждого пользователя, и специализированные вопросы, интересные профессионалам.

Развиваем проект Kids' Cyber Resilience для детей и подростков

Совместно с международными партнерами в 2023 году «Лаборатория Касперского» запустила программу «Киберустойчивость для детей» в странах Азиатско-Тихоокеанского региона. За прошедшее время она значительно расширилась, и теперь охватывает Вьетнам, Индонезию, Филиппины, Малайзию, Индию и Египет, а также страны СНГ.

В рамках проекта **Kids' Cyber Resilience** проводятся образовательные мероприятия для детей, родителей и педагогов, где все учатся безопасному поведению в цифровой среде. В 2024 году мы создали серию онлайн-тренингов по безопасному использованию искусственного интеллекта в обучении. Он предназначен специально для педагогов и родителей, чтобы они могли помочь молодежи ориентироваться в новых технологиях.

В 2026–2027 годах мы планируем запустить программу Kids' Cyber Resilience в России и странах СНГ, а также в ряде стран Ближнего Востока и Африки.

Формируем киберустойчивость общества

«Лаборатория Касперского» развивает ряд проектов, нацеленных на формирование ответственного отношения к технологиям через образование и культуру.

- **Курс** «IT-журналистика» — первый в России образовательный проект по ИБ для будущих журналистов. Журналисты играют ключевую роль в формировании общественного понимания цифровых рисков, киберугроз, возможностей новых технологий и принципов их безопасного использования. Чтобы повысить компетенции будущих медиаспециалистов в сфере IT и кибербезопасности, в 2025 году на базе Института медиа НИУ ВШЭ мы запустили курс «IT-журналистика». На нем студенты изучают кибербезопасность, IT-индустрию и знакомятся с особенностями работы с технологическими темами в медиа.
- **Книга** «Вирьё моё!» Хроники невидимых хакерских войн от Сыктывкара до Сингапура» стала еще одним способом рассказать широкой аудитории о мире кибербезопасности. Этот первый в России производственный роман про работу экспертов по информационной безопасности основан на реальных событиях и помогает широкой аудитории понять, как работают аналитики киберугроз, узнать природу киберрисков и механизмы противодействия им, сформировать у читателей более осознанное отношение к цифровым рискам.

Онлайн-игра «Дело 404»

Учим поколение Z кибербезопасности через игру

Проблема

Многие пользователи, особенно молодые, недооценивают цифровые угрозы, а традиционные форматы обучения кибербезопасности часто оказываются сложными и не вовлекающими.

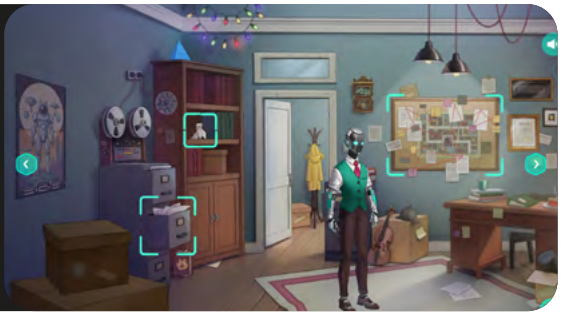
Что сделано

«Лаборатория Касперского» создала интерактивную онлайн-игру **«Дело 404»** на девяти языках с фокусом на поколении Z. В этой игре участники становятся кибердетективами, которые должны раскрыть захватывающие дела о киберпреступлениях. Пользователи решают задачи, основанные на реальных сценариях киберугроз: взломах, утечках данных, онлайн-преследовании и социальной инженерии.

Для продвижения проекта Компания реализовала ряд проектов совместно с партнерами — eSports командами NASR и Reckoning sports, а также Twitch Japan.

Результаты

- **>30 000** участников игры
- Повышение цифровой грамотности на практике
- Доступный и понятный формат обучения
- Формирование ответственного поведения в интернете



Развиваем образовательные программы для студентов и школьников

Комплексные курсы на платформе Kaspersky Academy

В 2025 году мы создали новую учебную платформу для вузов с доступом к курсам «Введение в кибербезопасность» и «Основы кибербезопасности», обновили их на русском и английском языках. Также запустили глобальный курс «Кибергигиена» — базовый уровень для всех, кто хочет защищать себя онлайн, и онлайн-курс для школьников и студентов по профессиям в ИТ и информационной безопасности.

Kaspersky Academy Alliance для колледжей России

Мы понимаем, что среднее профессиональное образование — важный этап, на котором формируются навыки будущих специалистов. Поэтому Компания запустила программу сотрудничества с колледжами, чтобы их студенты могли получать актуальное образование в области кибербезопасности.

Партнерства и стажировки для студентов

В Индонезии мы заключили соглашение с организацией PeaceGeneration Indonesia, направленное на повышение цифровой осведомленности молодежи. Также реализуются программы стажировок: в Индии студенты получают практический опыт работы в ИБ-сфере, а летний проект «Долина технологий» в России, который проводился в 2024 году, дал школьникам и студентам возможность поработать над реальными проектами Компании.

Работаем со школами и учителями

Просветительская работа в школах

С 2018 года «Лаборатория Касперского» ведет активную просветительскую работу в сфере информационной безопасности, направленную на учащихся российских школ, их родителей и учителей.

Так, эксперты Компании разработали учебный курс «Основы информационной безопасности» для учеников 7–11-х классов. Помимо самих школьников, его могут использовать учителя на уроках информатики и в рамках внеурочной деятельности, а также родители учащихся. В основе программы — материалы, накопленные за годы работы с преподавателями информатики и математики, а также с московскими школами в рамках сотрудничества с Департаментом образования и науки Москвы.

Курс регулярно обновляется, чему способствует в том числе работа Компании с десятью подшефными школами и колледжем, где регулярно проводятся офлайн-занятия. Топ-менеджеры «Лаборатории Касперского», в том числе и сам Евгений Касперский, выступают с лекциями для школьников и учителей в ГБОУ «Воробьевы горы».

в 10

подшефных школах проводят занятия эксперты «Лаборатории Касперского»

Кроме того, дважды в учебном году Компания проводит онлайн-курсы повышения квалификации для преподавателей математики и информатики из разных регионов России.

Вся просветительская деятельность «Лаборатории Касперского» осуществляется при поддержке и под патронатом Федерального института цифровой трансформации в сфере образования (ФИЦТО) Министерства просвещения Российской Федерации.

«Урок цифры»

ЦИФРОВАЯ ЭКОНОМИКА
НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ

Федеральный проект «Кадры для цифровой экономики»

Всероссийский образовательный проект «Урок цифры»

Реализуют Минпросвещения России, Минцифры России и АНО «Цифровая экономика» в партнерстве с ведущими российскими технологическими компаниями

С 2018 года «Лаборатория Касперского» выступает партнером всероссийского образовательного проекта «Урок цифры», который входит в федеральный проект «Кадры для цифровой экономики». Каждый год мы разрабатываем и выпускаем один тематический урок с интерактивным тренажером для школьников, родителей и учителей — эти уроки изучают в российских школах в течение трех недель.

>22 млн

прохождений набрали «Уроки цифры» от «Лаборатории Касперского» с 2018 года

Создавая новые уроки, мы стараемся не перегружать школьников сложной информацией, а, наоборот, сделать акцент на самом главном. Для нас важно подать материал легко и доступно, заинтересовать детей качественной анимацией и интерактивом.

Подробнее — на сайте проекта «Урок цифры»

Окружающая среда

ESG-направление

PUE 2
показатель энергоэффективности дата-центра «Лаборатории Касперского»

48%
доля продаж в электронных форматах в 2025 году

52%
собранных вещей передано людям в трудной жизненной ситуации

Как мы управляем охраной окружающей среды

Стремление к безопасности для нас не ограничивается цифровой средой, оно определяет и подход к охране окружающей среды. «Лаборатория Касперского» не оказывает прямого воздействия на экосистемы, однако мы на регулярной основе отслеживаем потребление ресурсов и стремимся популяризировать ответственное отношение к природе, чтобы укреплять экологическую безопасность, в том числе для будущих поколений.

Наш подход и ключевые воздействия

Охрана окружающей среды для «Лаборатории Касперского» — это последовательная системная работа. Мы отслеживаем прямые и непрямые воздействия нашей деятельности на окружающую среду и климат и стремимся свести их к минимуму.

Основные экологические воздействия Компании связаны с офисной деятельностью и ИТ-инфраструктурой. Мы потребляем воду и электроэнергию, образуем отходы (в том числе упаковку от физических продуктов), а также формируем углеродный след за счет непрямых источников — авиаперелетов, работы серверов и дата-центров, энергопотребления офисов, корпоративного транспорта и услуг, необходимых для разработки и распространения наших решений.

Для минимизации этих воздействий мы оптимизируем бизнес-процессы, стремимся поддерживать энергоэффективность офисов и серверной инфраструктуры, сокращаем потребление ресурсов и объемы образования отходов, возникающих при выпуске продукции на физических носителях.

Вопросы охраны окружающей среды находятся в зоне ответственности руководителей направлений «Лаборатории Касперского». Они разрабатывают и внедряют практические решения, которые помогают снижать экологическую нагрузку и поддерживать устойчивое развитие Компании.

Результаты отчетного периода

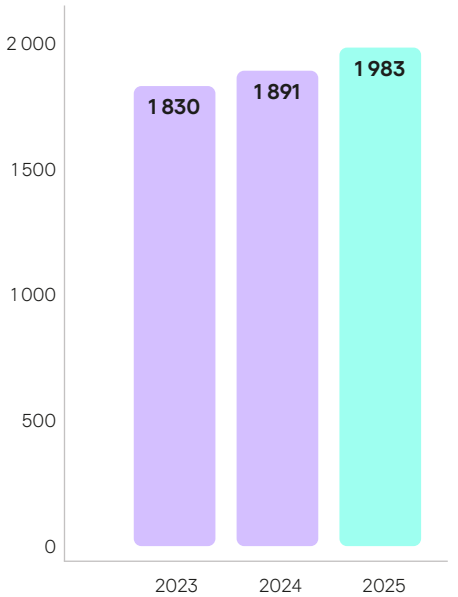
СОКБ 10, СОКБ 15

>3,8 млн рублей

инвестировала «Лаборатория Касперского» в мероприятия по охране окружающей среды в 2024–2025 годах

Мы строго соблюдаем требования природоохранного законодательства.
В 2024–2025 годах Компания не получала штрафов, нефинансовых санкций или жалоб, связанных с нарушениями в области охраны окружающей среды.

Общие расходы на охрану окружающей среды, тысяч рублей



Снижаем углеродный след

«Лаборатория Касперского» осознает влияние изменения климата и последовательно работает над сокращением углеродного следа своей деятельности.

В 2024–2025 годах мы продолжили анализировать климатическое воздействие Компании и оценивать возможности его снижения. В своей деятельности мы ориентируемся на ЦУР ООН, в том числе на ЦУР 13 «Борьба с изменением климата».

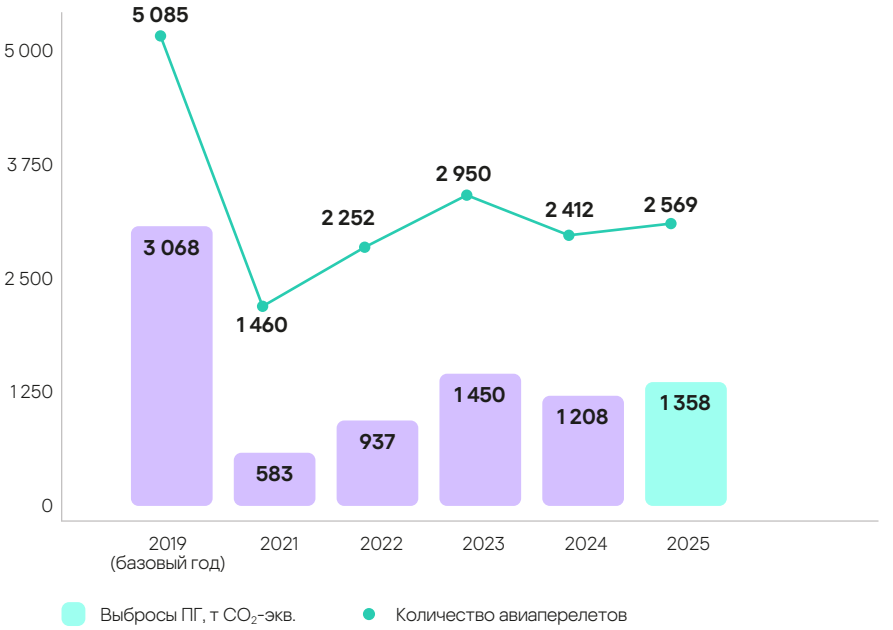
Уже сегодня мы предпринимаем практические шаги по снижению выбросов. В частности, используем энергоэффективное оборудование и технологии, а также стремимся сократить углеродный след, связанный с деловыми авиаперелетами и поездками.

Как мы управляем транспортными выбросами

GRI 305-3, GRI 303-5, СОКБ 8

Мы понимаем, что авиа- и автотранспорт существенно увеличивает климатическую нагрузку, поэтому мы целенаправленно сокращаем выбросы от сжигания топлива. За последние годы автопарк Компании был уменьшен до трех автомобилей, которые используются исключительно для срочных рабочих поездок.

Выбросы парниковых газов от авиаперелетов сотрудников Компании[1]



Мы также работаем над снижением углеродного следа от авиаперелетов. В 2024 году количество авиапоездок сотрудников Компании сократилось на 18,2% по сравнению с 2023 годом, а в 2025 году — на 12,9%. При этом в 2025 году нам удалось снизить объем выбросов в 2,3 раза по сравнению с базовым 2019 годом.

[1] Данные об авиаперелетах за 2020 год не приводятся в связи с приостановкой авиасообщения в 2020 году из-за пандемии COVID-19.

Повышаем энергоэффективность

Мы последовательно работаем над снижением энергопотребления офисов и дата-центров, сочетая технологические решения и ответственное управление инфраструктурой.

Наш подход к управлению энергопотреблением

СОКБ 18

Энергоэффективность для «Лаборатория Касперского» — это важная часть устойчивого развития и снижения экологического воздействия. Мы управляем энергопотреблением как в офисных помещениях, так и в центрах обработки данных (ЦОД), внедряя современные технологии, обновляя оборудование и оптимизируя процессы.

Штаб-квартира Компании расположена в московском бизнес-центре «Олимпия Парк», который имеет класс энергоэффективности «А» и сертифицирован по международному экологическому стандарту BREEAM[1]. Уже на этапе строительства здания были использованы энергоэффективные материалы и технологии.

В офисе мы применяем светодиодные осветительные приборы, датчики движения и автоматические регуляторы освещения, которые учитывают уровень естественного дневного света. Эти решения позволяют сокращать потребление электроэнергии без снижения комфорта для сотрудников. Аналогичное светодиодное освещение используется и на парковке бизнес-центра.

Текущее энергопотребление

GRI 302-1

В 2024–2025 годах общее потребление электроэнергии Компании несколько увеличилось. Это связано с естественным ростом бизнеса, расширением технологических мощностей в ЦОД и более активным использованием решений на базе искусственного интеллекта для работы с большими объемами данных. Такие технологии требуют значительных вычислительных ресурсов и поэтому крайне энергозатратны.

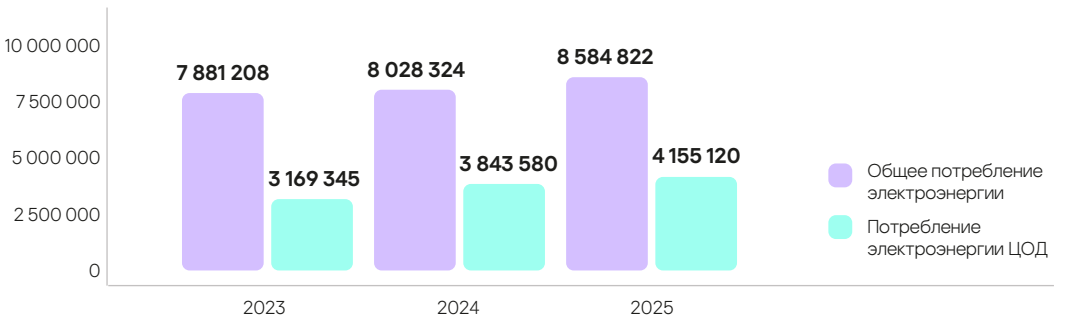
8 585 МВт • ч

общее потребление электроэнергии в 2025 году

При этом последовательная реализация программ энергоэффективности позволила снизить объем электроэнергии, потребляемой офисной частью Компании, несмотря на общее развитие и рост масштабов деятельности.

SASB TC-SI-130a.1, СОКБ 12

Энергопотребление в Компании[2], кВт • ч



[1] BRE Environmental Assessment Method — стандарт или метод оценки эффективности и экологичности зданий, разработанный британской компанией BRE Global.
[2] Границы раскрытия — московский офис АО «Лаборатория Касперского», включающий в себя и дата-центр Компании. По остальным офисам информация в отчетном периоде не собиралась.

Энергоэффективность дата-центров

GRI 302-4, SASB TC-SI-130a.3

PUE 2

показатель энергоэффективности ЦОД «Лаборатории Касперского»

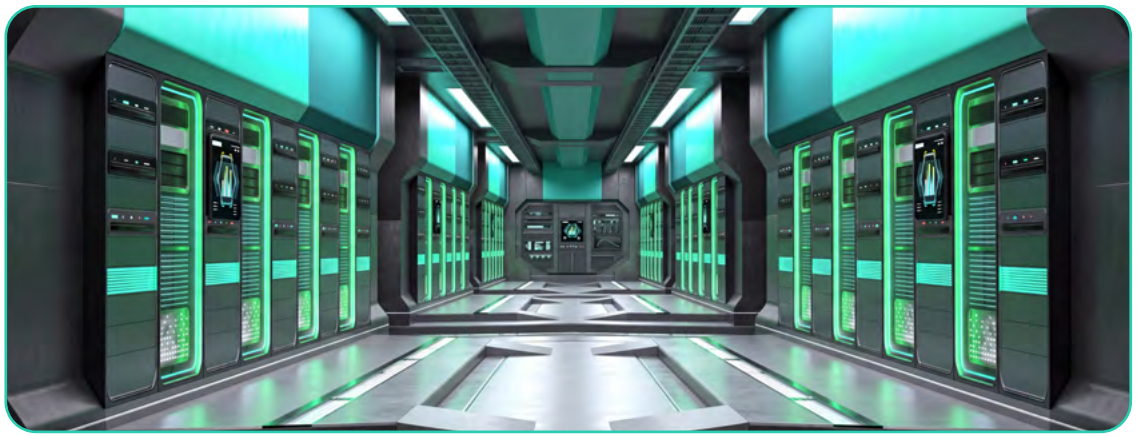
Дата-центры, или ЦОД, — один из главных источников энергопотребления в IT-отрасли. Энергия нужна для круглосуточной работы множества серверов и промышленных кондиционеров, обеспечивающих им необходимое охлаждение. «Лаборатория Касперского» использует собственный ЦОД, включающий 33 серверные стойки для поддержки пользовательской инфраструктуры и бэк-офиса, а также арендуемые дата-центры для нужд разработки.

Наш ЦОД подключен к двум независимым подстанциям. На случай аварийной ситуации в готовности находится дизельный генератор, позволяющий серверам продолжать работу около 10 часов после отключения всех прочих источников питания. Батареи источников бесперебойного питания (ИБП) могут поддерживать работу серверов в течение 30 минут, но основная их задача — это защита от кратковременных отключений и бесшовное переключение с городского электропитания на дизель-генератор. В серверной используется система газового пожаротушения, безопасная для окружающей среды.

Все электрооборудование регулярно проходит техосмотр. Один раз в две недели проводятся тестовые запуски генератора на холостом ходу, один раз в квартал — запуски под нагрузкой, а топливо в генераторе заменяется ежегодно. Обслуживание системы бесперебойного снабжения проводится ежеквартально и ежемесячно. При строительстве ЦОД применялись энергоэффективные технологии, в том числе интеллектуальные регуляторы температуры и датчики присутствия для освещения.

Снижение энергопотребления в ЦОД достигается также за счет обновления вычислительного оборудования. Мы заменяем устаревшее оборудование новым, которое в пересчете на единицу мощности выдает больше производительности, уменьшаем количество используемых кабелей и стоек, серверов, используя среды виртуализации и твердотельные накопители (SSD-диски). Мы перерабатываем старое компьютерное оборудование и передаем на благотворительность клавиатуры, ноутбуки, мониторы и телефоны.

Мы предъявляем высокие требования к инфраструктуре ЦОД и применяем энергоэффективные решения. В частности, в холодное время года используем режим естественного охлаждения дата-центра за счет температуры внешнего воздуха. Расширяем допустимый температурный диапазон работы серверов до 22–24 °C, организуем холодные и горячие воздушные коридоры. Чтобы предотвратить утечку газов, использующихся для охлаждения серверов, наши сотрудники два раза в день проверяют работу охлаждающего оборудования. В случае выявления утечки оборудование отключается, перекрывается подача хладагента и газ эвакуируется в специальный баллон.



Для оценки эффективности работы дата-центров мы используем коэффициент эффективности использования электроэнергии PUE (Power Usage Effectiveness), который рассчитывается как отношение общего энергопотребления дата-центра к энергопотреблению IT-оборудования.

В 2024–2025 годах значение PUE наших дата-центров составляло 2, тогда как средний мировой показатель в 2024 году был на уровне 1,56 (по оценке международной организации в области сертификации центров обработки данных Uptime Institute).

Оптимизируем использование воды

Мы ответственно подходим к использованию воды и стремимся сокращать ее потребление за счет технических и организационных решений.

Наш подход к использованию воды

GRI 303-1, GRI 303-2

В «Лаборатории Касперского» вода используется исключительно для обеспечения повседневной работы офиса и дата-центра. Мы получаем воду только из муниципальных систем водоснабжения и не осуществляем забор воды из природных источников или открытых водоемов. Сброс сточных вод в природные водные объекты также не производится.

Наш подход к использованию водных ресурсов основан на предотвращении потерь и поддержании надежной работы инженерных систем. Мы уделяем особое внимание техническому состоянию оборудования и своевременно модернизируем инфраструктуру, чтобы минимизировать риски аварий и нерационального использования воды.

Потребление воды и меры по его снижению

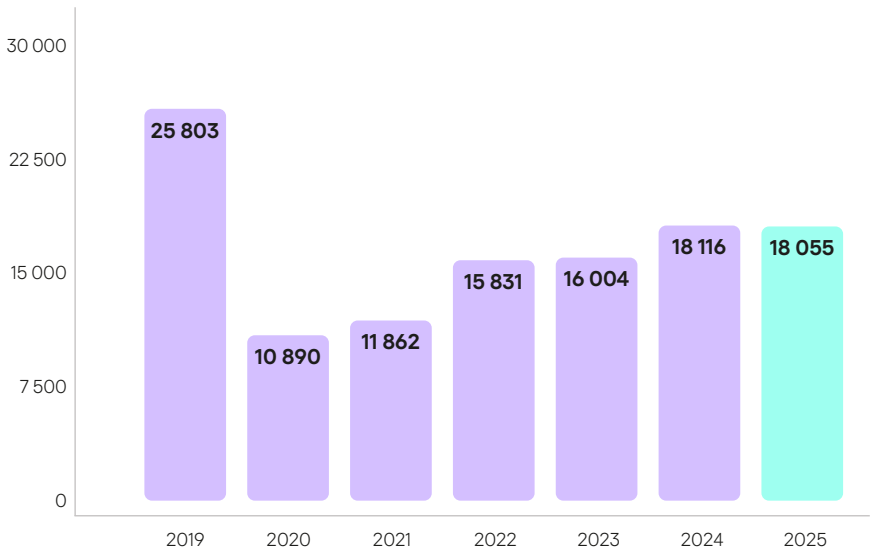
В 2024–2025 годах объем потребления воды в Компании несколько увеличился по сравнению с 2022–2023 годами. Это связано с постепенным изменением формата работы и ростом времени, которое сотрудники проводят в офисе вместо удаленной работы. При этом текущий уровень водопотребления по-прежнему остается существенно ниже базового показателя 2019 года.

Для снижения потребления воды и предотвращения потерь мы реализуем комплекс технических мер, в том числе:

- проводим регулярную экспертизу состояния запорно-регулирующей арматуры;
- периодически выполняем анализ воды для контроля состояния трубопроводов;
- поддерживаем необходимый запас запасных частей и оборудования. Это позволяет оперативно устранять неисправности и минимизировать потери воды в случае аварийных ситуаций.

GRI 303-3, СОКБ 1, SASB TC-SI-130a.2

Объем забора воды[1], куб. м



В 2026–2027 годах мы планируем проработать возможность установки дополнительных отсекающих устройств на магистральных трубопроводах. Такое решение позволит быстрее и точнее локализовать возможные протечки, сократить зону отключения и уменьшить объем воды, подлежащий сливу при проведении ремонтных работ.

[1] Границы раскрытия — московский офис АО «Лаборатория Касперского», включающий в себя и дата-центр Компании (основной источник водопотребления в организации). По остальным офисам информация в отчетном периоде не собиралась. Вода в бизнес-операциях используется для хозяйственно-бытовых целей в офисах Компании, поэтому учет водопотребления — общий. Территории расположения офисов компании не относятся к регионам водного стресса.

Управляем образованием отходов

Мы стремимся сокращать объем отходов и обеспечивать ответственное обращение с ними на всех этапах нашей деятельности — от офисной работы до выпуска продуктов.

Наш подход к управлению отходами

GRI 306-1, GRI 306-2

Управление отходами в «Лаборатории Касперского» — это сочетание сокращения их образования, раздельного сбора и ответственной утилизации.

Значительная часть отходов в Компании связана с повседневной деятельностью офиса и выпуском продуктов на физических носителях. Именно на этих направлениях мы фокусируем основные усилия по сокращению экологической нагрузки.

Виды отходов и обращение с ними

В офисах Компании образуются в основном бытовые и офисные отходы, а также отдельные виды отходов повышенной опасности, например батарейки и электронные устройства. В московском офисе внедрена система раздельного сбора: установлены контейнеры для бумаги, пластика, стекла, металла и смешанных отходов, а в принтерных комнатах — отдельные емкости для макулатуры, пластиковых крышек, батареек, аккумуляторов и электронных сигарет.

Сбор, транспортировку и передачу отходов на переработку или утилизацию мы доверяем специализированным компаниям. При этом все контрагенты проходят проверку на соответствие требованиям законодательства. Отходы I и III классов опасности перед отправкой на утилизацию или захоронение проходят частичное обезвреживание.

GRI 306-3, GRI 306-4, GRI 306-5, СОКБ 5, СОКБ 6

Образование отходов[1], тонн

Показатели	2023	2024	2025
Общее образование отходов на объектах Компании, в том числе:	**225,6**	**353,7**	**410,8**
■ **I класс** (чрезвычайно опасные, неразлагаемые: пестициды, асбест, приборы, содержащие ртуть)	0,1	0,3	0,3
■ **II класс** (высокоопасные, разлагаются более 10 лет: инсектициды, фунгициды, свинец, мышьяк, аккумуляторы, пиротехника)	0	0	0
■ **III класс** (умеренно опасные, разлагаются от трех до десяти лет: гербициды, лакокрасочные материалы, моющие средства, шампуни, дезодоранты, мобильные телефоны)	0,7	0,4	0,7
■ **IV класс** (малоопасные, разлагаются до трех лет: азотные удобрения, ДВП, ДСП, полиэтиленовая пленка, зеркала, резиновые перчатки и обувь, одноразовая посуда, бытовая техника)	219,4	353,0	409,9
■ **V класс** (практически неопасные, разлагаются до трех лет: продукты питания, натуральные ткани и изделия из них, бумажные и картонные изделия)	5,4	0	0
Направлено на захоронение	225,1	352,9	409,9
Направлено на утилизацию	0,2	0,4	0,7
Направлено на обезвреживание	0,3	0,3	0,3

[1] Учитываются отходы московского офиса, включая ЦОД, а также отходы в результате бизнес-операций.

Работаем над сокращением образования отходов

«Лаборатория Касперского» последовательно внедряет практики, позволяющие уменьшать объем отходов еще на этапе их образования.

Меры по сокращению образования отходов в Компании:

- анализ и отбор поставщиков, предлагающих продукцию в перерабатываемой и экологичной упаковке;
- отказ от использования избыточных и функционально необоснованных предметов в операционной деятельности;
- использование многоразовой посуды и качественных материалов с длительным сроком службы;
- повышение экологичности сувенирной и рекламной продукции Компании за счет выбора устойчивых материалов и решений.

В частности, мы последовательно снижаем использование пластика в производстве сувенирной продукции. Вместо пластиковых пакетов мы закупаем пакеты из высокопрочных материалов, а также многоразовые холщовые сумки.

В 2026–2027 годах Компания планирует внедрить программы по повышению экологической грамотности сотрудников, а также пересмотреть внутренние регламенты, с тем чтобы снизить потребление бумаги и одноразовых материалов. Также будет рассмотрена возможность использования оборудования с более длительным сроком службы и модернизации существующего, чтобы уменьшить объем утилизируемой техники.

Оптимизируем упаковку

Значимую долю отходов в мире формирует упаковка товаров. Чтобы сократить ее объемы, мы последовательно сокращаем выпуск продуктов на физических носителях, уменьшая толщину коробок и пространство на поддонах, развиваем коммуникацию на упаковке, чтобы облегчить переработку и сократить, и продвигаем цифровую дистрибуцию. В 2025 году доля коробочных продуктов Компании в продажах решений для домашних пользователей оставалась на уровне 8,8%.

Полный отказ от выпуска продукции на физических носителях для нас пока невозможен: часть покупателей по-прежнему предпочитает CD или DVD, в основном в силу привычки. В отдельных регионах, включая страны Африки, это связано с отсутствием стабильного доступа к интернету. Для таких продуктов мы используем компактные упаковочные решения с минимально возможным содержанием пластика.

[1] Point-of-Sales Activation — продукт, который активируется в точке продаж.

Форматы продуктов «Лаборатории Касперского» на физических носителях

Боксы, лифлеты и конверты

Картонные коробки или тонкие конверты с вложенным флаером, на котором напечатан активационный код коробки с компакт-диском, содержащим продукт

DVD-коробки

Пластиковые боксы без диска, внутри которых находится листовка с кодом (в странах франкоязычной Африки в коробку дополнительно вкладывается диск)

Пластиковые карточки

Код скрыт под защитным слоем, активируется после стирания покрытия

POSA POR

Используется как витринная карточка из тонкого картона, сам код не расположен на карте, а печатается на чеке при покупке

POSA[1]-карты

Картонные носители с кодом (открытым или скрытым), используемые как экономичный формат

Увеличиваем долю продаж в электронных форматах

В целом доля электронных лицензий и цифровых форматов в течение 2022–2025 годов показала тенденцию к росту, темпы которого различаются в зависимости от региона. Компания активно переводит действующую клиентскую базу на цифровые лицензии через различные механизмы. В России, Латинской Америке и Северной Европе их доля уже приблизилась к 85–90%.

36% выручки от продажи решений для домашних пользователей приходится на реаквизицию (продление), когда спустя год после покупки новой лицензии они снова возвращаются на сайт за приобретением следующей. В период с 2024 по 2025 год 6% таких лицензий перешли в цифровой канал — после первой покупки в розничном магазине потребители на следующий год оформляли покупку онлайн.

Нашим партнерам мы предлагаем переходить к покупке онлайн-лицензий, а дистрибьюторам — распространять лицензии через собственные сайты, что также упрощает доступ к зарубежным рынкам.

Внедряем более экологичную упаковку

В 2024–2025 годах Компания провела комплексную экологическую трансформацию ретейл-упаковки. Обновленные форматы стали более экономичными. Так, бокс теперь на 50% тоньше и на 20% легче, чем предыдущая версия, а конверт — на 80% компактнее. Мы также полностью отказались от внутреннего картонного вкладыша, что позволило снизить потребление картона и краски, сократить объемы перевозок и оптимизировать хранение у дистрибьюторов.

52%
доля продаж в коробочных решениях в 2025 году

48%
доля продаж в электронных форматах в 2025 году

Используем специальную маркировку

В соответствии с требованиями регламента об упаковке и упаковочных отходах **PPWR (Package and Packaging Waste Regulation)** «Лаборатория Касперского» размещает на упаковке информацию, помогающую потребителям правильно сортировать и утилизировать использованные материалы, а также соблюдает требования расширенной ответственности производителей **(EPR[1])** во всех регионах присутствия.

На всех упаковочных материалах Компании нанесены обязательные **PAP/PP символы**. Это международные коды маркировки, используемые для идентификации состава упаковки и облегчения ее сортировки и переработки. **PAP** обозначает изделия из бумаги и картона, **PP** — изделия из полипропилена (пластика).

Наша продукция зарегистрирована в национальных системах **EPR** и ежегодно отчитывается по их правилам. Во Франции используется маркировка **Triman**, в Германии и Португалии — **Green Dot**, в Испании — **Symbol for Recycling** с цветовой кодировкой, а для итальянского рынка применяется знак **Disposal IT PRP** (Preparazione per il Riutilizzo e il Riciclo) с подробными рекомендациями по утилизации.

Кроме того, с 2025 года продукция, поставляемая на рынок Италии, дополнительно маркируется сертификатом Лесного попечительского совета **FSC[2]**, который подтверждает использование упаковочных материалов из ответственно управляемых лесов.

Экономим бумагу, развивая цифровые процессы

Мы сокращаем использование печатных материалов и передаем устаревшие баннеры, плакаты и фотопанели на утилизацию. Для экономии бумаги Компания с конца 2022 года активно использует электронный документооборот (ЭДО) с внешними контрагентами.

В 2024 году по ЭДО было подписано на 75% больше документов, чем годом ранее, а в 2025 году — еще на 20% больше.

Более 50% контрагентов уже работают с нами в цифровом формате, что покрывает свыше 40% бухгалтерских документов. В 2025 году это позволило сэкономить более 20 000 рублей.

В перспективе мы планируем внедрить систему внутреннего кадрового электронного документооборота.

[1] Extended Producer Responsibility — принцип экологического регулирования, в рамках которого производители и импортеры несут ответственность за экологические аспекты своей продукции на протяжении всего жизненного цикла, включая сбор, переработку и утилизацию упаковки и отходов после использования.

[2] Forest Stewardship Council (FSC) — это международная некоммерческая неправительственная организация, которая занимается продвижением ответственного управления лесами во всем мире.

Развиваем экологическую культуру

Мы последовательно формируем экологичные привычки у сотрудников и поддерживаем инициативы, которые помогают заботиться об окружающей среде.

«Лаборатория Касперского» развивает экологическую культуру через системные программы и повседневные практики. Мы рассказываем сотрудникам о принципах разумного потребления, поддерживаем их инициативы и вовлекаем в экологические проекты местные сообщества.

Сотрудники активно участвуют в экологических акциях Компании. Те, кому близок экологичный образ жизни, вступают во внутреннее сообщество Green like Mirodi, в котором можно обсуждать разные идеи по улучшению офиса. Мы регулярно проводим лекции, мастер-классы и экскурсии, посвященные защите окружающей среды, а репортажи с мероприятий публикуем во внутренней сети, чтобы с ними могли ознакомиться все желающие.

В 2024–2025 годах основной фокус, помимо экологического просвещения внутри Компании, был направлен на укрепление партнерств с благотворительными фондами «Второе дыхание» и «Природа и люди».

Осознанно относимся к вещам

С фондом «Второе дыхание» мы сотрудничаем с 2022 года. В нашем офисе был установлен контейнер для сбора одежды и текстиля, а в 2024 году мы обновили его дизайн, сделав более ярким. На контейнере появились пояснения о том, какие вещи принимаются, и в каком виде их нужно сдавать, а также наглядная схема пути вещей: от офиса до сортировки, благотворительности, переработки или утилизации. Кроме того, мы стали регулярно делиться статистикой, чтобы сотрудники видели реальный эффект от своих действий.

Эти изменения дали результат. В 2024 году наши сотрудники собрали 1 535,8 кг вещей (на 9,1% больше, чем годом ранее).

Способы обращения с собранной одеждой и текстилем в 2025 году, %

Помощь людям в трудной жизненной ситуации	52
Переработка	36
Утилизация	10

В 2025 году было собрано 1 803,2 кг вещей, из которых уже 52% фонд смог использовать для прямой помощи людям. Рост этого показателя особенно важен для нас: он показывает, что сотрудники все более осознанно подходят к сбору вещей.

>3 тонн

вещей собрали сотрудники Компании за 2024–2025 годы

Совместно с фондом «Второе дыхание» мы также проводили творческие мероприятия для сотрудников:

- мастер-класс по переделке старых вещей — эксперт фонда показал, как можно придать одежде новый вид и носить ее дольше;
- мастер-классы на корпоративных днях детей в 2024 и 2025 годах, где участники вместе с детьми создавали открытки и интерьерные украшения из вторичных материалов.

В 2025 году мы реализовали еще один важный проект вместе с фондом — переработали старые брендированные вещи Компании. Более 1 500 футболок и свитеров были переделаны мастерицами фонда в уникальные косметички и чехлы для ноутбуков. Коллекция была представлена на корпоративной новогодней ярмарке в декабре 2025 года во благо фонда «Живи».

Помогаем сохранять редкие виды животных

ПРИРОДА И ЛЮДИ

В партнерстве с фондом «Природа и люди» мы поддерживаем проекты по сохранению редких животных и экосистем.

В 2024 году «Лаборатория Касперского» участвовала в проекте «Сохраняем каланов». В июле мы помогли провести морскую экспедицию на остров Уруп и другие острова Курильской гряды, чтобы оценить состояние популяций калана и разработать предложения по организации их охраны. Ученые прошли 175 км береговой линии и зафиксировали более 530 каланов. Результаты подтвердили устойчивость популяции и важность защиты этих территорий от антропогенного воздействия.

Также в 2024 году мы организовали экстренный сбор средств для помощи фонду в закупке корма для голубого песца на острове Медный. В ту зиму популяция этих животных могла полностью исчезнуть из-за критической нехватки пищи. Наши сотрудники собрали более 100 000 рублей, Компания удвоила эту сумму, а затем дополнительно перечислила еще 300 000 рублей в рамках новогоднего сбора фонда.

В 2025 году мы снова поддержали проект «Сохраняем песцов на острове Медный». В ходе экспедиций на островах Охотского моря специалисты оценили численность популяций, а на остров Медный было доставлено 600 кг корма и установлены две новые подкормочные площадки, чтобы помочь животным пережить зиму. Компания также поддержала новогодний сбор фонда на проект по сохранению лошади Пржевальского, пожертвовав более 200 000 рублей.

Фонд также регулярно делится результатами своей работы с сотрудниками Компании, в том числе в формате лекций в рамках внутренних мероприятий, встреч клуба путешественников «Лаборатории Касперского» и других клубов по интересам.

420 кг

техники сдано на экологическую переработку в 2024–2025 годах

>1 300 книг

собрано и передано новым читателям

Делаем экологию частью офисной жизни

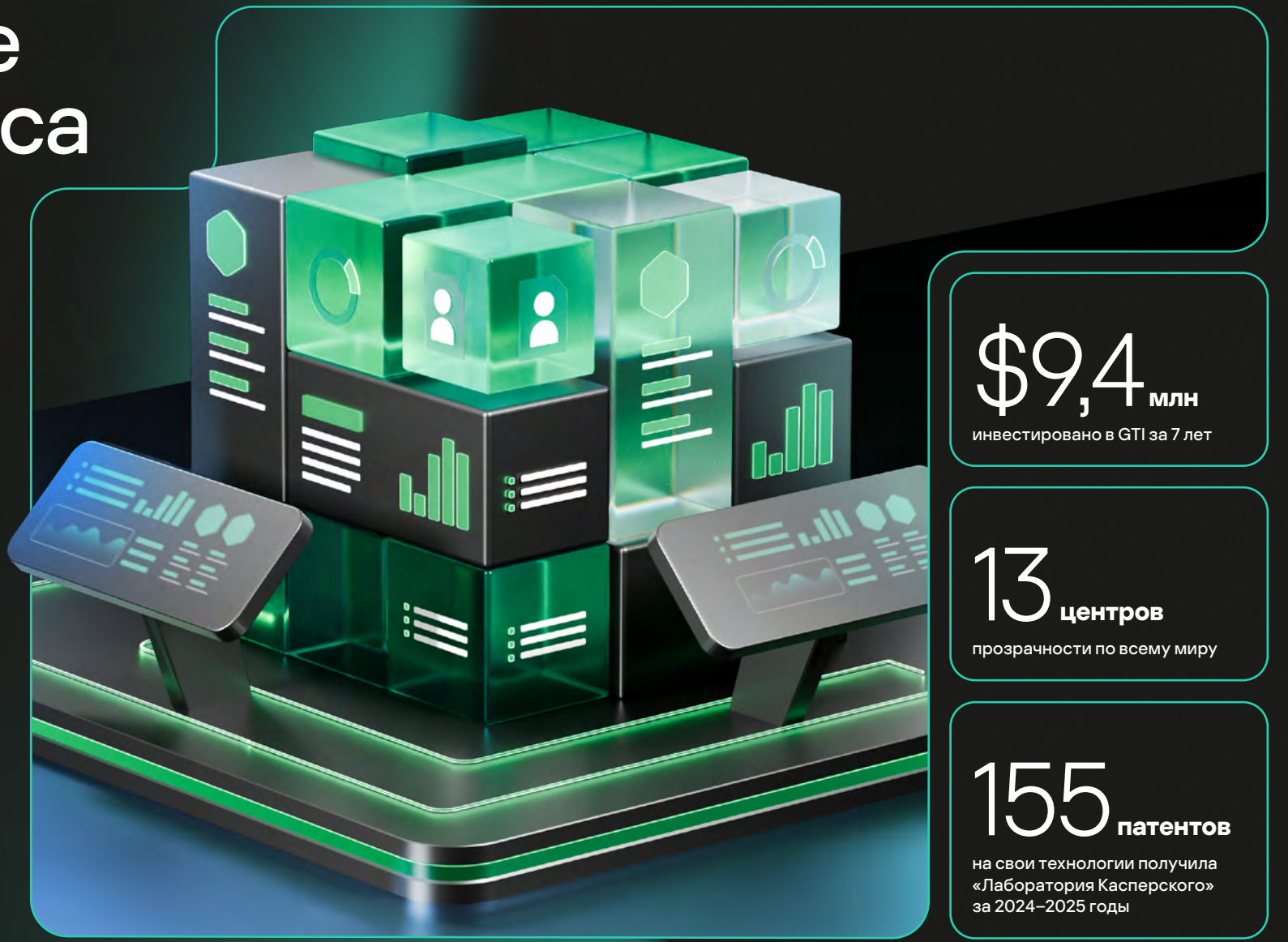
Мы уверены, что экологическая культура формируется из небольших, но регулярных действий, поэтому продолжаем создавать для наших работников условия, в которых осознанный выбор становится привычным.

Ежегодно мы проводим экологическую неделю, когда наши сотрудники собирают ненужную электронику, книги, одежду и передают все это партнерам «Лаборатории Касперского». В 2024 году на экологичную утилизацию нашему партнеру «Петромакс» было передано 170 кг электронной техники, а в сельские библиотеки в рамках социального экопроекта Re:Books — более 400 книг.

В 2025 году сотрудники собрали уже 250 кг электроники и 514 книг. Кроме того, мы провели отдельную акцию по сбору книг для благотворительного фестиваля в пользу фонда «Живи», на которой было собрано более 400 экземпляров.

Осенью 2025 года у нас появилась зона быстрой зарядки для электромобилей. Это позволило большему числу сотрудников пользоваться электромобилями и заряжать их в удобном формате.

Ответственное ведение бизнеса



$9,4 млн
инвестировано в GTI за 7 лет

13 центров
прозрачности по всему миру

155 патентов
на свои технологии получила «Лаборатория Касперского» за 2024–2025 годы

Соблюдение прав человека

Соблюдение прав сотрудников, клиентов, местных сообществ и других заинтересованных сторон является базовым и неотъемлемым принципом деятельности и лежит в основе корпоративной культуры и ответственного ведения бизнеса в «Лаборатории Касперского».

GRI 406-1

GRI 2-23, GRI 2-24

«Лаборатория Касперского» руководствуется принципами Глобального договора ООН, Резолюцией Генеральной Ассамблеи ООН о целях устойчивого развития, Парижским соглашением от 12 декабря 2015 года, Международным биллем о правах человека, включающим Всеобщую декларацию прав человека, Конвенцию о защите прав человека и основных свобод, одобренными ООН «Руководящими принципами предпринимательской деятельности в аспекте прав человека», а также соответствующим национальным и региональным законодательством стран присутствия.

Кроме того, «Лаборатория Касперского» подписала пакт Европейской комиссии об искусственном интеллекте[1] (далее — Закон об ИИ). Подписание пакта отражает стремление Компании содействовать разумному и ответственному использованию технологий ИИ, тем самым «Лаборатория Касперского» признает их важность в области кибербезопасности.

Подписав соглашение, мы взяли на себя три основных обязательства:

- принять стратегию управления ИИ, чтобы способствовать его внедрению внутри самой Компании таким образом, чтобы в будущем соответствовать регулированию в этой сфере;
- определить системы ИИ, которые могут быть отнесены к категории высокого риска в соответствии с Законом об ИИ;
- повышать уровень осведомленности в области ИИ сотрудников Компании и других лиц, работающих с такими системами от ее имени, с учетом их технических знаний, опыта, образования и подготовки, а также контекста, в котором будут использоваться системы ИИ.

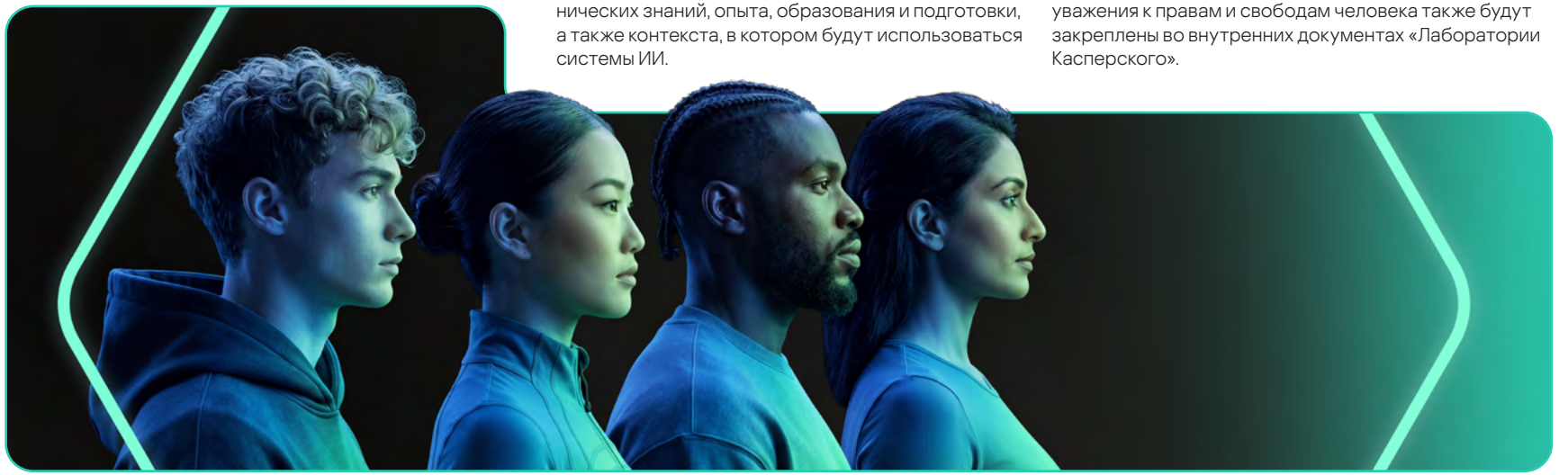
«Лаборатория Касперского» не приемлет любых форм дискриминации, использования детского, рабского или принудительного труда и ожидает аналогичных решений от своих контрагентов по всей цепочке поставок.

Такая позиция Компании зафиксирована во внутренней политике, отражающей руководящие принципы ведения деятельности в странах ее присутствия. Принципы уважения к правам и свободам человека также будут закреплены во внутренних документах «Лаборатории Касперского».

0

случаев дискриминации в Компании в отчетном периоде

Компания строго соблюдает международное и локальное законодательство, опираясь на «Руководство по социальной ответственности» ISO 26000-2010 и международный стандарт AA1000 (AccountAbility Principles, Stakeholder Engagement Standard).



[1] Закон об искусственном интеллекте Евросоюза должен полностью вступить в силу в середине 2026 года.

Соблюдение прав человека в деятельности Компании

Основные права человека	Документы, которыми руководствуется Компания	Подходы Компании в области соблюдения прав человека	Группы заинтересованных сторон, на которые Компания может влиять в сфере прав человека	Результаты отчетного периода
Право на жизнь, свободу, неприкосновенность частной жизни, личную и семейную тайну	■ Конституция Российской Федерации, ст. 20, 22, 23 ■ Применимые законы в странах присутствия «Лаборатории Касперского», в том числе: – GDPR[1]; – Международный стандарт по информационной безопасности ISO/IEC 27001; – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; – PIPL[2]; – CCPA[3]; – LGPD[4]; – PDPD[5]	Один из приоритетов Компании — обеспечить защиту данных наших клиентов по всему миру при помощи внутренних систем и процедур по безопасности. Мы не используем данные в целях, отличающихся от целей сбора данных	■ Пользователи ■ Сотрудники ■ Уязвимые с точки зрения информационной безопасности группы ■ НКО	0 серьезных нарушений законодательства о персональных данных 0 значительных утечек данных
Право на труд	■ Конституция Российской Федерации, ст. 37 ■ Трудовой кодекс Российской Федерации ■ Правила внутреннего трудового распорядка ■ Политика в области охраны труда ■ Гайдлайн по благотворительным проектам ■ Положение о комитете по устойчивому развитию ■ Применимые законы в странах присутствия «Лаборатории Касперского»	Для «Лаборатории Касперского» сотрудники — самый ценный актив. Мы стремимся, чтобы людям в Компании было комфортно и интересно, чтобы они могли работать продуктивно, чувствовали себя защищенными, могли развиваться сами и развивать Компанию. «Лаборатория Касперского» поддерживает деятельность некоммерческих организаций, помогающих людям с ограниченными возможностями здоровья в трудоустройстве и социализации, а также оказывающих им юридическую поддержку	■ Сотрудники ■ Уязвимые с точки зрения информационной безопасности группы ■ НКО	5 691 человек — общая численность персонала на конец 2025 года (+11,3% к численности на конец 2024 года) 10% — текучесть персонала в 2025 году (–5 п. п. к текучести за 2024 год) Пять НКО поддержала Компания за отчетный период, деятельность которых направлена на трудоустройство людей с инвалидностью Компания приняла участие в десяти мероприятиях по инклюзивному трудоустройству (бизнес-завтраки, ярмарки вакансий, менторская программа) Один информационный проект о профессиональном и личном пути сотрудников с инвалидностью и тех, кто воспитывает детей с инвалидностью, опубликовала Компания: https://kasperskystories.ru/

[1] Европейский регламент по защите данных (EU General Data Protection Regulation).
[2] Закон КНР о защите персональных данных (Personal Information Protection Law of the People's Republic of China).
[3] Закон штата Калифорния о защите персональных данных потребителей (California Consumer Privacy Act).
[4] Общий закон о защите данных Бразилии (Lei Geral de Proteção de Dados).
[5] Закон Вьетнама о защите персональных данных (Personal Data Protection Decree).

Основные права человека	Документы, которыми руководствуется Компания	Подходы Компании в области соблюдения прав человека	Группы заинтересованных сторон, на которые Компания может влиять в сфере прав человека	Результаты отчетного периода
Право на благоприятную окружающую среду	■ Конституция Российской Федерации, ст. 42 ■ Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» ■ Положение о Комитете по устойчивому развитию ■ Гайдлайн по благотворительным проектам ■ Применимые законы в странах присутствия «Лаборатории Касперского»	Ответственное отношение к окружающей среде — одна из важнейших ценностей «Лаборатории Касперского». Мы снижаем негативное воздействие на природу за счет экономного потребления ресурсов, хорошо организованных бизнес-процессов и ответственного отношения к источникам энергии для дата-центров и офиса	■ Сотрудники ■ Местные сообщества ■ Пользователи ■ НКО	>50% контрагентов уже подключены к ЭДО[1] и работают с нами в цифровом формате. >3 тонн вещей сдали на благотворительность, переработку и утилизацию сотрудники Компании за 2024–2025 годы. 420 кг электротехники передали на утилизацию >1 300 книг собрали и передали в сельские библиотеки за два года >500 000 рублей направили на закупку корма для голубого песца на о. Медный в 2024 году 200 000 рублей пожертвовали на проект по сохранению лошади Пржевальского в 2025 году В 2024 году Компания поддержала реализацию проекта фонда «Природа и люди» по сохранению каланов
Право на образование	■ Конституция Российской Федерации, ст. 43 ■ Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 04.08.2023) «Об образовании в Российской Федерации» ■ Положение о комитете по устойчивому развитию ■ Гайдлайн по благотворительным проектам ■ Применимые законы в странах присутствия «Лаборатории Касперского»	Мы поощряем стремление сотрудников к новым знаниям, постоянно совершенствуем внутренние образовательные программы и добавляем новые. Мы организовываем совместные образовательные проекты с некоммерческими организациями, которые помогают людям с ограниченными возможностями здоровья, пенсионерам, жертвам домашнего насилия и другим людям, оказавшимся в сложной жизненной ситуации. «Лаборатория Касперского» создает собственные обучающие программы, нацеленные на взаимодействие с учебными заведениями и аудиторией, которой необходимо дополнительное образование. Мы вкладываем ресурсы в развитие как школьников и студентов, так и уже опытных специалистов кибербезопасности, нуждающихся в повышении квалификации	■ Сотрудники ■ Пользователи ■ Уязвимые с точки зрения информационной безопасности группы ■ НКО	Компания взаимодействует более чем с 200 вузами в 45 странах мира ~50 вузов из разных стран присоединились к программе Academy Alliance за два года. В 2024 году совместно с фондом «Синдром любви» Компания представила первое в России методическое пособие по цифровой грамотности для людей с синдромом Дауна. 800 стажеров пришли в «Лабораторию Касперского» в рамках программы стажировок SafeBoard за 10 лет. >350 выпускников программы стажировок SafeBoard продолжают работать в Компании >22 млн прохождений набрали «Уроки цифры» от «Лаборатории Касперского» с 2018 года. >3 000 пользователей из более чем 50 стран — аудитория тренингов Kaspersky Expert Training

[1] Электронный документооборот.

Основные права человека	Документы, которыми руководствуется Компания	Подходы Компании в области соблюдения прав человека	Группы заинтересованных сторон, на которые Компания может влиять в сфере прав человека	Результаты отчетного периода
Право на охрану здоровья и медицинскую помощь	■ Конституция Российской Федерации, ст. 41 ■ Положение о выплатах компенсационного и стимулирующего порядка ■ Применимые законы в странах присутствия «Лаборатории Касперского»	Забота о здоровье и благополучии сотрудников — важная составляющая социальной политики «Лаборатории Касперского». Социальный пакет, доступный всем сотрудникам[1] Компании в России, включает широкий спектр медицинских услуг. Мы также продвигаем идеи активного и здорового образа жизни среди сотрудников	Сотрудники	0 случаев травматизма среди сотрудников в 2024–2025 годах 0 случаев профессиональных заболеваний у сотрудников Компании выявлено в 2024–2025 годах Сотрудники «Лаборатории Касперского» в России и их дети до 16 лет включительно охвачены корпоративной программой ДМС[2] Две лекции с врачами-онкологами в формате вопросов-ответов об онкологических заболеваниях, необходимости своевременных чекапов и сдачи анализов
Право на защиту от дискриминации	■ Конституция Российской Федерации, ст. 19, 29 ■ Руководящие принципы предпринимательской деятельности в аспекте прав человека ■ Внутренняя политика «Лаборатории Касперского», отражающая руководящие принципы ведения деятельности в странах ее присутствия	Мы не приемлем и не поощряем дискриминацию любого рода в деятельности Компании	■ Сотрудники ■ Пользователи ■ Партнеры	0 случаев дискриминации в Компании в отчетном периоде

[1] Для сотрудников с временными трудовыми договорами и работающих на условиях неполной занятости доступен сокращенный соцпакет. В Компании около 0,1% таких сотрудников.
[2] Добровольное медицинское страхование.

Корпоративное управление

Наш бизнес строится на уважении к интересам клиентов, партнеров и рынка в целом. Мы поощряем открытое взаимодействие, стремимся повышать качество раскрытия информации и считаем, что доверие и репутация — ключевые активы Компании и основа устойчивого развития.

Ключевые принципы

- Обеспечение прозрачности корпоративного управления
- Соблюдение антикоррупционной политики за счет недопущения случаев ее нарушений
- Высокий уровень правовой поддержки, связанной с охраной и защитой интеллектуальной собственности
- Снижение рисков по цепочке поставок

Наш подход к корпоративному управлению

Мы дорожим репутацией Компании и стремимся укреплять доверие через ответственное управление, добросовестные практики и высокие стандарты во всех аспектах своей деятельности. Ключевые принципы и правила, которые формируют культуру делового общения и профессионального поведения, зафиксированы во внутренних политиках «Лаборатории Касперского», а также в обязательном для прохождения сотрудниками онлайн-курсе «Основы корпоративной этики».

Совет директоров

GRI 2-10, GRI 2-11, GRI 2-13, СОКБ 48

Высший орган управления в «Лаборатории Касперского» — совет директоров. Он отвечает за ключевые решения, принимает глобальные политики и стратегии, которые имплементируются во все компании внутри группы. В текущем составе совета директоров два человека. Все они находятся на постоянном контракте более пяти лет. Независимых членов в совете директоров нет, только исполнительные.

Кандидатов в совет директоров назначают действующие члены совета.

В нашей Компании нет постоянного председателя совета директоров. Он избирается на каждое заседание совета, у него нет специальных полномочий.

Ответственность за экономические, социальные и экологические воздействия устойчивого развития делегирована руководителю департамента корпоративных коммуникаций Денису Зенкину.

Управляющий совет

Управляющий совет определяет конкретные стратегические и тактические шаги для операционного развития Компании и структуру управления группой, а также утверждает назначения топ-менеджеров.

Роль генерального директора Евгения Касперского в управлении определяющая, поскольку он одновременно крупнейший акционер холдинговой компании, член совета директоров и управляющего совета.

Коллективные знания высшего руководящего органа

GRI 2-17

Для повышения информированности и компетенций высшего органа управления в вопросах устойчивого развития представители совета директоров и управляющего совета регулярно участвуют в обучающих мероприятиях с приглашением внешних экспертов.

Оценка деятельности высшего органа управления

GRI 2-18

Регулярная оценка деятельности совета директоров и управляющего совета проводится ежегодно собранием акционеров «Лаборатории Касперского». На основе этой оценки выполняются реструктуризации, улучшающие операционное управление Компанией. Критерии оценки деятельности управляющих органов по вопросам надзора за управлением воздействиями Компании на экономику, окружающую среду и социальную сферу в отчетном периоде не внедрялись.

Деловая этика и противодействие коррупции

«Лаборатория Касперского» соблюдает законодательство и требования регуляторов по всему миру, последовательно развивая культуру деловой этики, прозрачности и нулевой терпимости к коррупции.

Как мы соблюдаем антикоррупционную политику

GRI 2-24

Основополагающий принцип деятельности Компании заключается в том, что мы не приемлем никаких форм подкупа или коррупции как по отношению к нам, так и со стороны Компании и ее сотрудников, а также не участвуем ни в каких формах неэтичных поощрений или платежей.

«Лаборатория Касперского» соблюдает применимое антикоррупционное законодательство Российской Федерации, стран своего присутствия, а также международное антикоррупционное законодательство, включая закон США «О борьбе с коррупцией за рубежом» (Foreign Corrupt Practices Act, FCPA) и закон Великобритании «О борьбе со взяточничеством» (UK Bribery Act 2010). При этом в штаб-квартире приоритет отдается законодательству Российской Федерации, а в зарубежных офисах — местному антикоррупционному законодательству.

Базовые принципы противодействия коррупции закреплены в антикоррупционной политике, принятой в 2012 году. Она была переведена на 30 языков и опубликована на официальном сайте Компании.

GRI 205-1, GRI 2-25, GRI 2-26

В «Лаборатории Касперского» регулярно проводится оценка рисков, связанных с коррупцией.

За соблюдение антикоррупционной политики отвечает руководство Компании, а координацию и методическую поддержку по приведению внутренних норм и процедур в соответствие с требованиями политики осуществляет комплаенс-специалист.

Каждый сотрудник и представитель Компании, которому стали известны факты или признаки нарушения антикоррупционной политики и применимого антикоррупционного законодательства, обязан сообщить об этом. При желании это можно сделать анонимно.

0

судебных решений по вопросам нарушений антикоррупционного законодательства в отношении Компании, сотрудников и партнеров

Компания предоставляет несколько каналов для информирования:

- обращение к непосредственному руководителю или, если сообщение касается именно его действий, — к вышестоящему руководителю;
- обращение на горячую линию Компании по телефону **8 (800) 700-88-11**;
- сообщение информации по адресу электронной почты: nocorrupt@kaspersky.com;
- непосредственное обращение к комплаенс-сотруднику или его представителям;
- связь с комплаенс-сотрудником Компании по номеру 3000 для сотрудников в московском офисе и **+7 (495) 797-87-00** (доп. 3000) — для звонка по городскому телефону.

Антикоррупционное обучение и информирование

GRI 203-2, GRI 205-3

«Лаборатория Касперского» ежегодно информирует своих сотрудников об антикоррупционной политике и соответствующих процедурах. При заключении договоров с контрагентами мы интегрируем в договоры антикоррупционную политику.

Для обучения сотрудников Компания разработала специальный онлайн-курс, посвященный борьбе со взяточничеством и коррупцией. Этот курс включает знакомство с базовыми принципами и основными направлениями антикоррупционной политики Компании, в числе которых:

- цели антикоррупционного законодательства;
- важность соблюдения норм российских и зарубежных законов о взяточничестве и противодействии коррупции;
- модели поведения, которые приводят к нарушению законов по борьбе с коррупцией;
- необходимость проявления осмотрительности в деловых отношениях с третьими лицами;
- механизмы внутреннего контроля, определяющие деятельность сотрудников в соответствии с антикоррупционной политикой.

Антикоррупционный курс рассчитан на 30–40 минут обучения. Результаты тестирования по итогам курса заносятся во внутреннюю систему «Лаборатории Касперского». В отчетном периоде обучение прошли все сотрудники Компании — от высшего менеджмента до младших специалистов.

В 2026 году мы планируем обновить материалы антикоррупционного тренинга и продолжить внедрение лучших практик противодействия коррупции в деятельность Компании.

100%

сотрудников и партнеров информированы об антикоррупционной политике

0

подтвержденных случаев коррупции в Компании

Как мы предотвращаем конфликт интересов

GRI 2-15

В «Лаборатории Касперского» действует политика декларирования участия сотрудников и членов органов управления в иных компаниях в качестве учредителей, участников, акционеров или членов органов управления. Такое участие допускается только при условии его прозрачного раскрытия и при наличии предварительного согласия совета директоров или управляющего совета.

Совмещение участия в органах управления или капитале других организаций без соответствующего одобрения рассматривается как недопустимый конфликт интересов и запрещено корпоративными документами Компании.

В отчетном периоде случаев участия членов высших органов управления Компании в других организациях без согласия совета директоров или управляющего совета не выявлено.

Защита доверия пользователей

«Лаборатория Касперского» создает среду, в которой пользователи, клиенты и партнеры могут быть уверены в безопасности и надежности продуктов и услуг, предоставляемых Компанией.

Клиентский сервис

Доверие пользователей и клиентов — основа долгосрочного развития для «Лаборатории Касперского». Компания выстраивает все процессы так, чтобы взаимодействие с ней было удобным и понятным на каждом этапе: от выбора и использования продукта до общения со службой поддержки и получения обратной связи. В основе нашего подхода — уважение к клиентам, внимательное отношение к их потребностям и стремление быстро и точно реагировать в любой ситуации.

Взаимодействие с потребителями

Для эффективного взаимодействия с потребителями, клиентами и поставщиками в «Лаборатории Касперского» действует форма обратной связи на официальных сайтах Компании:

www.kaspersky.ru/about/contact
для русскоязычных пользователей

www.kaspersky.com/about/contact
для международных пользователей

Для различных типов обращений, включая вопросы по покупке продуктов, техническую поддержку и партнерство, предусмотрены отдельные каналы и специализированные команды. Такой подход позволяет оперативно разобраться в каждой ситуации и предложить наиболее подходящее решение.

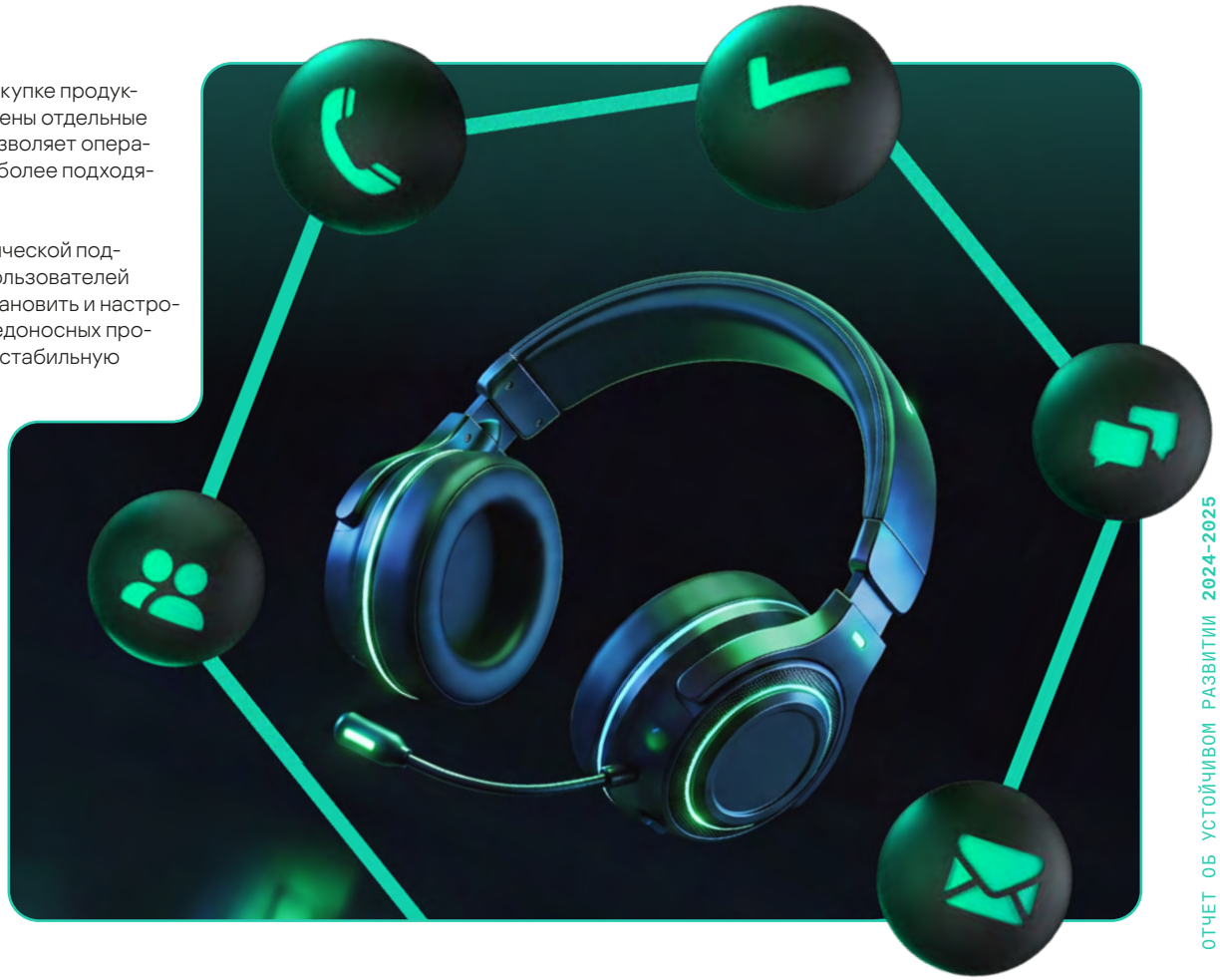
Клиенты Компании имеют доступ к круглосуточной технической поддержке, в том числе в формате удаленной помощи для пользователей потребительских продуктов. Специалисты помогают установить и настроить решения, провести проверку системы на наличие вредоносных программ и устранить технические неполадки, обеспечивая стабильную и бесперебойную работу защиты.

Работа с жалобами

GRI 2-25

Если у клиента возникают вопросы, претензии или предложения, он может обратиться через форму на сайте, по электронной почте, телефону или другим доступным каналам. Все обращения фиксируются и отслеживаются: это позволяет не только оперативно реагировать на каждую ситуацию, но и выявлять повторяющиеся проблемы, чтобы устранять их системно, а не точечно.

Команда, работающая с жалобами, в первую очередь стремится понять суть обращения и причины, вызвавшие беспокойство клиента, а затем предлагает понятное, прозрачное и обоснованное решение. Цель такого подхода — не просто формально закрыть запрос, а восстановить доверие и вернуть клиенту уверенность в качестве сервиса и продуктов Компании.



Защита данных

GRI 3-3

Мы уважаем право наших клиентов на конфиденциальность и защищаем их данные. Наша цель — исключить утечки данных в «Лаборатории Касперского», а также помочь нашим клиентам противостоять им с помощью наших решений.

>1 835

запросов на обработку данных пользователей в 2024–2025 годах

GRI 418-1

0

случаев утечки данных пользователей в отчетном периоде

Ключевые задачи

- Обеспечение защиты данных клиентов по всему миру с использованием лучших практик в области информационной безопасности и учетом локальных нормативных актов
- Оперативное реагирование на запросы клиентов по вопросам обработки и защиты их данных
- Предотвращение несанкционированного доступа и утечек данных пользователей

Приоритетные направления в сфере защиты данных в 2024–2025 годах

- Внедрение обновленных требований по информационной безопасности в сервисах Компании
- Обеспечение защиты от угроз, связанных с цепочкой поставок
- Обеспечение безопасности сервисов Компании с использованием ИИ
- Расширение защиты критичных сервисов от DDoS-атак
- Запуск новой программы Bug Bounty[1]

Наш подход к защите данных

SASB TC-SI-230-a.2

«Лаборатория Касперского» делает все возможное для обеспечения защиты данных своих клиентов по всему миру. В современном мире данные являются ценным активом для компаний, поэтому их сохранность и целостность имеют первостепенное значение. Мы защищаем персональную информацию[2] клиентов от несанкционированного доступа и изменений, применяя лучшие в своем классе технологии, а также комплекс технических и организационных мер безопасности.

Компания постоянно отслеживает изменения законодательства в области обработки и защиты персональных данных в различных юрисдикциях и реализует специальные проекты, направленные на приведение процессов и систем в соответствие с актуальными требованиями.

В большинстве стран мира применяется рискориентированный подход к формированию мер защиты персональных данных. Вместе с тем в ряде государств перечень таких мер установлен в явном виде и обязателен к исполнению. Указанные требования формализованы и применяются к сервисам Компании. В их числе, в частности, следующие технические меры:

- ограничение доступа к данным;
- своевременная установка обновлений и патчей безопасности;
- антивирусная защита;
- регистрация и мониторинг событий;
- сетевая защита;
- шифрование данных;
- обеспечение отказоустойчивости и резервного копирования.

Дополнительно реализуются организационные меры по защите данных, включая:

- ограничение объема собираемых персональных данных;
- анонимизацию данных;
- разработку защищенных продуктов и оперативное устранение выявленных уязвимостей;
- использование цифровых сертификатов;
- раздельное хранение данных на нескольких серверах.

Как мы защищаем данные по всему миру и предотвращаем их утечки

SASB TC-SI-220a.1

Мы руководствуемся ключевыми принципами работы с данными согласно Европейскому регламенту по защите данных, принятому в 2016 году. Именно этот законодательный акт предписывает фундаментальные технические и организационные меры, которые также признаются эталонными в других юрисдикциях. Кроме того, мы выполняем требования международного стандарта по информационной безопасности ISO/IEC 27001 и учитываем требования законов о защите персональных данных разных стран, в числе которых PIPL, CCPA, LGPD, PDPD, федеральный закон № 152-ФЗ и др.

Персональные данные хранятся не дольше, чем это необходимо для достижения целей их обработки, либо в сроки, установленные применимым законодательством. Актуальная информация о странах обработки, порядке доступа и сроках хранения данных приведена в действующей версии политики конфиденциальности Компании.

[1] Программа поощрения поиска ошибок и уязвимостей в программном обеспечении, которую, как правило, объявляют разработчики приложений и сетевых платформ, чтобы обнаружить проблемы в безопасности своих продуктов. Обычно в рамках программы энтузиасты получают денежное вознаграждение за сообщение об ошибках, которые могут быть использованы злоумышленниками; иногда в качестве поощрения может выступать доступ к платному онлайн-сервису или признание в профессиональном сообществе.

[2] Персональная информация — любая информация, относящаяся к физическому лицу, включая Ф. И. О., номера телефонов, адрес, IP-адрес, адрес электронной почты и т. д.

Пять ключевых принципов работы с данными клиентов

- Законность и прозрачность обработки данных для субъектов данных
- Легитимность целей обработки
- Отказ от сбора избыточных данных
- Соблюдение предельных сроков хранения данных
- Надежная защита данных

Мы стремимся к полному предотвращению инцидентов в сфере информационной безопасности. В отчетном периоде не было зафиксировано нарушений законодательства о персональных данных, а также случаев утечки информации. Такие результаты достигнуты благодаря системной работе по обучению сотрудников, внедрению современных технологий защиты информации и стандартизации процессов обработки данных.

В течение отчетного периода мы актуализировали требования к обработке данных и провели их адаптацию с учетом законодательства различных юрисдикций.

Актуальная информация, включая данные о количестве удовлетворенных запросов пользователей, отражается в нашем отчете прозрачности. Документ находится в открытом доступе, регулярно обновляется и публикуется каждые шесть месяцев.

Обучаем правилам работы с данными

В «Лаборатории Касперского» действует программа повышения осведомленности в области информационной безопасности для сотрудников, работающих непосредственно с данными клиентов. По состоянию на 2025 год программа охватывает всех действующих сотрудников Компании.

Обучение проходит в формате сочетания онлайн- и офлайн-активностей и направлено на формирование устойчивых навыков безопасного поведения. В рамках программы сотрудники изучают правила работы с персональными данными и коммерческой тайной, основы безопасного использования сервисов искусственного интеллекта, а также проходят практические занятия по распознаванию фишинговых и мошеннических атак и реагированию на них.

С 2025 года программа также распространяется на новых аутсорсеров и подрядчиков, имеющих доступ к информационным системам «Лаборатории Касперского», что позволяет обеспечить единый подход к вопросам информационной безопасности для всех участников рабочих процессов.

Оцениваем риски

Мы применяем рискориентированный подход к защите данных наших пользователей. Оценка рисков проводится на всех ключевых этапах работы — при внедрении новых систем, разработке решений и расследовании инцидентов. В каждом случае мы заранее анализируем возможные риски, связанные с обработкой данных клиентов, и принимаем меры для их минимизации.

Требования GDPR и регионального законодательства основаны на оценке рисков, которым могут подвергаться пользователи. Дополнительно снижать репутационные и финансовые риски для Компании нам помогает применение международного стандарта ISO/IEC 27001.

Предотвращаем утечки данных клиентов

GRI 418-1 | SASB TC-SI-220-a.1 | SASB TC-SI-230-a.1 | SASB TC-SI-220-a.3

За соблюдение принципов и процедур в области безопасности данных в Компании отвечает Privacy Team.

В рамках внедрения требований GDPR в Компании создана и работает команда Privacy Team, в которую входят сотрудники подразделений ИТ, R&D, ИБ и интеллектуальной собственности. В 2016 году Privacy Team привела в соответствие европейскому регламенту все процессы, связанные с обработкой данных. Сегодня она обеспечивает выполнение функций обработки данных в таких направлениях, как консультирование, организационные вопросы и контроль.

Начиная с 2019 года «Лаборатория Касперского» ежегодно подтверждает соответствие своих систем обработки данных требованиям международного стандарта ISO/IEC 27001, что свидетельствует о высоком уровне защиты информации. В отчетном периоде область аудита информационных систем была существенно расширена: на регулярной основе проводились аудиты ISO/IEC 27001 и SOC 2 второго типа, а в 2025 году дополнительно был проведен внешний аудит на соответствие требованиям Cybersecurity Regulatory Framework (CRF) Королевства Саудовская Аравия.

Область сертификации распространяется на область обработки данных «Лаборатории Касперского» «Доставка вредоносных и подозрительных файлов и статических данных об активности с помощью инфраструктуры Kaspersky Security Network (KSN), их безопасное хранение и доступ в Kaspersky Lab Distributed File System (KLDFS) и к базе данных KSNBuffer».

Сертификация распространяется на сервисы обработки данных, размещенные в дата-центрах, расположенных в Цюрихе, Франкфурте-на-Майне, Глаттбурге, Торонто, Москве и Пекине.

0
серьезных нарушений законодательства о персональных данных и значительных утечек

0
убытков в результате судебных разбирательств из-за нарушения конфиденциальности за отчетный период

46
внутренних аудитов ИБ проведено в 2024–2025 годах

Развиваем систему учета процессов обработки данных

Мы продолжаем развивать систему учета процессов и сервисов обработки данных, созданную командой разработчиков «Лаборатории Касперского» в 2023 году. Система позволяет отслеживать, какие сервисы обрабатывают данные клиентов, в рамках каких бизнес-процессов они используются, кто выступает контроллером (оператором) и процессором (обработчиком) данных, а также какие именно данные хранятся, на каком правовом основании, в каком объеме, в течение какого срока и в каких странах осуществляется их обработка.

В отчетном периоде были актуализированы и доведены до сервисов требования к обработке персональных данных, а также обеспечен контроль их выполнения.

Наши планы на 2026 год

- Мониторинг изменений в законодательстве о персональных данных в различных странах и приведение наших процессов в соответствие с актуальными требованиями
- Выставление обновленных требований по обработке и защите данных ко всем сервисам, в которых обрабатываются данные клиентов, и контроль их выполнения
- Проведение консультаций для команд по обновленным требованиям и практикам работы с данными
- Проведение аудитов эффективности сервисов в области обработки и защиты данных пользователей

Защита интеллектуальной собственности

Мы постоянно разрабатываем и внедряем перспективные решения в области кибербезопасности, а также регулярно патентуем наши изобретения и инновационные технологии.

Как мы охраняем и защищаем интеллектуальную собственность

Один из важнейших компонентов развития и стабильности нашего бизнеса — права на интеллектуальную собственность. Мы охраняем свои разработки, а также уважаем права других компаний на их технологии и решения.

Задача

Охрана и защита прав на продукты, решения и технологии

Решения

Получаем патенты в разных юрисдикциях

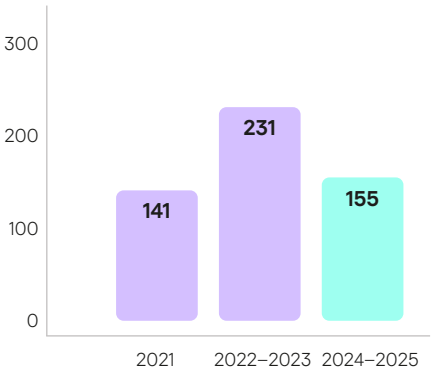
SASB TC-SI-520-a.1

«Лаборатория Касперского» последовательно закрепляет за собой охраняемые государством исключительные права на результаты своей интеллектуальной деятельности. В случае их нарушения мы готовы отстаивать свои права в судебном порядке, что помогает поддерживать принципы справедливости и законности в бизнес-среде.

За 2024–2025 годы Компания получила 155 патентов на свои технологии в разных юрисдикциях. В последние годы фокус патентования сместился в сторону B2B-продуктов и KasperskyOS и охватывает, помимо прочего, технологии машинного обучения и использование больших языковых моделей (LLM) для решения задач в области информационной безопасности. Кроме того, в отчетном периоде мы увеличили количество заявок на патенты, связанные с дизайном наших продуктов, включая пользовательские интерфейсы.

Охрана и защита интеллектуальной собственности (ИС) являются неотъемлемой частью деятельности «Лаборатории Касперского» с 2005 года. За это время мы выстроили и оптимизировали процессы получения правовой охраны для любых результатов интеллектуальной деятельности. Важным достижением Компании стало отсутствие проигранных судебных процессов по патентным спорам, инициированным против нас патентными троллями[1].

Патенты, полученные на продукты «Лаборатории Касперского», шт.



155 патентов

на свои технологии получила «Лаборатория Касперского» за 2024–2025 годы

[1] Физическое или юридическое лицо, чей бизнес состоит исключительно в получении лицензионных платежей за использование принадлежащих ему патентов, без попыток реализовать запатентованные изобретения на практике.

Наряду с защитой собственных разработок мы уделяем большое внимание предотвращению рисков, связанных с неправомерным использованием ИС третьих лиц внутри Компании. В том числе это касается использования стороннего программного кода. Для этого внедрены соответствующие политики, проводится тщательная проверка лицензий и ведется контроль за соблюдением всех применимых требований и норм.

При необходимости мы всегда готовы отстаивать свои права в суде — это одна из наших ключевых стратегических позиций. Мы используем все доступные законные механизмы защиты, не прибегая при этом к необоснованным схемам урегулирования. Наша цель — справедливое и правовое разрешение споров с учетом интересов всех сторон.

Так, в апреле 2024 года мы завершили двухлетний патентный спор в США с нашим прямым конкурентом — антивирусной компанией Webroot. Спор был урегулирован на условиях, устраивавших обе стороны, что позволило нам избежать возможных негативных сценариев его дальнейшего развития.

Развиваем культуру интеллектуальной собственности

Накопленный опыт и экспертиза позволяют нам не только эффективно охранять и защищать собственные инновации, но и вносить вклад в развитие культуры интеллектуальной собственности в Компании.

Важная часть этой работы — обучение и информирование сотрудников. Каждый новый сотрудник «Лаборатории Касперского» проходит специальный ознакомительный тренинг, который позволяет ему получить базовое понимание принципов интеллектуальной собственности и правил работы с ней.

В январе 2025 года мы также запустили специализированный курс по патентам для сотрудников технических подразделений. Он помогает разобраться в основах патентования и понять, как интеллектуальные права охраняют инновации и способствуют развитию бизнеса. В рамках курса сотрудники, вовлеченные в разработку новых продуктов, получают не только базовые знания по патентному праву, но и информацию о внутренних процедурах Компании, связанных с охраной интеллектуальной собственности.

В отчетном периоде мы существенно увеличили количество публикаций на внутреннем медиаресурсе, посвященных не только патентованию, но и другим объектам ИС.

Кроме того, мы уделяем много внимания поддержке сотрудников, обучающихся в высших учебных заведениях и желающих использовать интеллектуальную собственность «Лаборатории Касперского» в своих научных исследованиях. Каждому такому сотруднику предоставляется необходимая экспертная поддержка для реализации исследовательских инициатив при одновременной защите критически важной информации.

Наши планы на 2026 год

- Расширение географии правовой охраны изобретений за счет дополнительных юрисдикций и увеличение общего количества подаваемых патентных заявок
- Мониторинг изменений правового ландшафта с целью оперативного пересмотра локальных нормативных актов в области ИС, а также для формирования новых документов, направленных на решение актуальных проблем
- Развитие программ обучения и информирования сотрудников, включая создание ресурсов и инструкций по вопросам интеллектуальной собственности для сотрудников — студентов высших учебных заведений. Это поможет обеспечить соблюдение правил и политик Компании
- Повышение уровня автоматизации внутренних процессов в области интеллектуальной собственности

Поддерживаем высокий уровень внутренней эффективности

По мере ежегодного расширения круга задач в области интеллектуальной собственности особое значение приобретает повышение эффективности и автоматизация процессов. За 2024–2025 годы в этом направлении был реализован ряд инициатив.

1. Мы продолжаем развивать автоматизированную систему для анализа программного обеспечения и других объектов с open-source- и free-лицензиями. В отчетном периоде был разработан и внедрен отдельный модуль, который позволяет эффективно определять лицензионные условия и формировать сведения об авторских правах на ПО с открытым исходным кодом, используемое в продуктах Компании. Это позволило существенно ускорить правовую экспертизу наших продуктов и сервисов и обеспечить соответствие лучшим мировым практикам работы с программным обеспечением с открытым исходным кодом.
2. Была пересмотрена процедура публикации open-source-проектов, предоставляющих сообществу разработчиков доступ к нашим технологиям. Для команд разработки был подготовлен структурированный и понятный гайдлайн, что позволило снизить вероятность ошибок при публикации кода, а также сократить избыточную коммуникацию с подразделением, ответственным за вопросы интеллектуальной собственности.
3. В отчетном периоде был внедрен LLM-ассистент, который помогает ускорить анализ патентов из иностранных юрисдикций и оптимизировать работу в этом направлении.

Global Transparency Initiative

Наша цель — предоставить инструменты и условия для валидации целостности и надежности продуктов нашим корпоративным клиентам, партнерам и регуляторам.

Proven.
Transparent.
Independent.

Что такое Global Transparency Initiative

Global Transparency Initiative (GTI, Глобальная инициатива по информационной открытости) — это система мер, направленных на повышение прозрачности и надежности продуктов, процессов разработки и бизнес-процессов «Лаборатории Касперского». Благодаря GTI клиенты, партнеры и регуляторы могут получить доступ к информации об архитектуре продуктов, работе с данными и процедурам обеспечения безопасности, включая просмотр исходного кода в специализированных Центрах прозрачности. А обратная связь от внешних экспертов помогает нам совершенствовать процессы и поддерживать высокий уровень зрелости решений.

Как возникла и развивалась GTI

Global Transparency Initiative была запущена в 2018 году как ответ на запросы регулирующих органов и клиентов, которые интересовались деталями работы наших продуктов, включая обработку и хранение данных. Сегодня GTI — это комплексная система, объединяющая независимые аудиты, анализ исходного кода, образовательные инициативы и развитие инфраструктуры обработки данных.

В рамках GTI Компания:

- внедрила независимый анализ исходного кода, обновлений и правил обнаружения угроз;
- внедрила независимую оценку безопасной разработки и управления рисками в цепочке поставок;
- открыла сеть Центров прозрачности (Transparency Centers) по всему миру;
- усовершенствовала программу Bug Bounty;
- перенесла часть инфраструктуры для хранения и обработки подозрительных файлов в дата-центры в Швейцарии;
- начала публиковать отчеты о запросах от правоохранительных органов и государственных структур;
- развивала программы повышения компетенций в области безопасности IT-инфраструктуры, такие как Cyber Capacity Building Program.

В 2025 году «Лаборатория Касперского» отметила семилетие Глобальной инициативы по информационной открытости. За этот период GTI превратилась в полноценную систему обеспечения прозрачности.

Результаты работы GTI за семь лет

>$9,4 млн
инвестиций в развитие GTI за 7 лет

2
дата-центра в Цюрихе

13
Центров прозрачности по всему миру

67
визитов в Центры прозрачности

$97 770
выплачено за 77 репортов об ошибках в рамках Bug Bounty

Как работает GTI

Основные элементы GTI

1. Доступ к исходному коду для клиентов и регуляторов

Важный элемент системы — независимая верификация кода продуктов «Лаборатории Касперского». Кроме того, ряд заинтересованных лиц может получить информацию об исходном коде основных продуктов Компании и наших принципах работы с данными.

2. Сотрудничество с экспертным сообществом

Мы приглашаем независимых экспертов из разных стран для проверки наших систем и продуктов, что добавляет еще больше уверенности в их надежности.

3. Образовательная деятельность

Образовательные инициативы Компании в рамках GTI направлены на повышение осведомленности пользователей и партнеров о важности безопасности в цифровом мире.

Как мы обеспечиваем прозрачность наших продуктов и бизнес-процессов

Задача

Укрепление доверия общества к продуктам и деятельности Компании

Чтобы укрепить доверие клиентов, партнеров и регуляторов, мы постоянно развиваем инфраструктуру GTI, раскрываем данные о наших процессах, проходим аудиты, сертификации и совершенствуем стандарты безопасности.

13
Центров прозрачности
работают по всему миру

2
независимых аудита SOC 2 и на соответствие ISO 27 001 ежегодно

Запущен курс по GTI для партнеров

Основные решения

Развиваем инфраструктуру обработки данных

В 2018 году «Лаборатория Касперского» запустила процесс переноса обработки и хранения подозрительных и вредоносных файлов в два дата-центра в Швейцарии, в которых действуют строгие правила защиты данных. Благодаря этому сегодня в Цюрихе обрабатываются данные, которые пользователи из стран Европы, Северной и Латинской Америки, Ближнего Востока, а также ряда стран Азиатско-Тихоокеанского региона на добровольной основе передают в облачную систему Kaspersky Security Network.

Расширяем сеть Центров прозрачности

Центры прозрачности позволяют нашим корпоративным клиентам, партнерам и государственным регуляторам, отвечающим за кибербезопасность, изучить исходный код продуктов Компании и узнать больше о внутренних процессах. Первый центр был открыт в Цюрихе в 2018 году. Всего за семь лет мы создали 13 Центров прозрачности — в Бразилии, Италии, Японии, Малайзии, Нидерландах, Руанде, Саудовской Аравии, Сингапуре, Испании, Швейцарии, Турции, Колумбии и Южной Корее. Три из них были открыты в 2024–2025 годах.

Итоги работы GTI за 2024–2025 годы

3
новых Центра прозрачности открыто — в Стамбуле, Боготе и Сеуле

7
ревью продуктов Компании в Центрах прозрачности

>$15 000
выплачено за 18 репортов об ошибках в рамках Bug Bounty

Проходим независимую оценку

«Лаборатория Касперского» регулярно получает независимую оценку и подтверждает безопасность своих внутренних процессов. С 2019 года системы управления данными Компании проходят сертификацию в соответствии со стандартом ISO/IEC 27001:2022 и аудит SOC 2.
В 2025 году система управления информационной безопасностью «Лаборатории Касперского» была вновь успешно сертифицирована по стандарту ISO/IEC 27001:2022, что подтвердило ее безопасность.

Также в 2024 и 2025 годах Компания успешно прошла аудит SOC 2 второго типа. Он показал, что внутренние средства контроля «Лаборатории Касперского», которые обеспечивают регулярное автоматическое обновление антивирусных баз, работают эффективно, а процесс разработки и выпуска антивирусных баз защищен от несанкционированного вмешательства.

В 2024 и 2025 годах году мы дважды успешно прошли аудит SOC 2 второго типа

Собираем данные об уязвимостях через программу Bug Bounty

С марта 2018 года «Лаборатория Касперского» получила 77 сообщений о незначительных уязвимостях в рамках программы Bug Bounty, устранила их и на сегодняшний день выплатила независимым исследователям вознаграждение на общую сумму $97 770. Максимальный размер награды за критические уязвимости — $100 000.

С 2022 года Компания проводит свою публичную программу вознаграждения за ошибки на платформе Yogosha. Также мы поддерживаем проект Disclose.io, который представляет собой безопасную площадку для исследователей уязвимостей, обеспокоенных возможными негативными юридическими последствиями своих раскрытий.

77
репортов об ошибках получено за 7 лет

$97 770
выплачено за репорты

Учим, как оценивать уровень кибербезопасности

Наша образовательная программа Cyber Capacity Building помогает сотрудникам частных и государственных компаний, а также университетов развивать навыки в области оценки уровня безопасности IT-инфраструктуры. В рамках программы наши специалисты предоставляют рекомендации по аудиту кода, созданию процедур для обработки уязвимостей и методике фаззинга кода[1].

За отчетный период тренинг прошли представители нескольких организаций, включая Национальное агентство кибербезопасности Таиланда и Босфорский университет (Стамбул).

В 2025 году Cyber Capacity Building Program была отмечена Всемирной конференцией по вопросам интернета (WIC) как выдающийся пример вклада, вносимого в создание сообщества с общим будущим в киберпространстве

Публикуем отчеты о прозрачности

Наша миссия — защищать пользователей от киберугроз, поэтому мы оказываем поддержку партнерам, международным организациям и правоохранительным органам в борьбе с киберпреступностью. Мы регулярно обрабатываем запросы и с 2020 года публикуем отчетность: в каких юрисдикциях получаем такие запросы, сколько из них удовлетворены и сколько отклонены. Для этого внутри Компании существует процесс по обработке таких запросов и, в частности, четкие критерии для их юридической проверки.

«Лаборатория Касперского» каждые полгода раскрывает количество запросов от полиции на предоставление информации о пользовательских данных, экспертизы и технической информации для расследования угроз. При этом мы не предоставляем доступ к инфраструктуре Компании, включая инфраструктуру по работе с данными, никаким третьим сторонам[2].
С такой же периодичностью мы рассказываем о запросах от наших собственных пользователей об их персональных данных и о том, как мы с ними работаем, где они хранятся и т. д.

1 Метод тестирования программного обеспечения, когда программе отправляют заведомо неверные данные, анализируют реакцию и за счет этого обнаруживают ошибки.
2 Подробнее о принципах работы с запросами можно прочитать в наших отчетах о прозрачности.

Наш вклад в развитие этичного и безопасного использования ИИ в кибербезопасности

Искусственный интеллект позволяет эффективнее выявлять и нейтрализовать новые киберугрозы, однако его использование несет риски в области приватности, безопасности данных и соблюдения прав пользователей. В 2024–2025 годах «Лаборатория Касперского» активизировала свою деятельность по разработке и продвижению этических норм использования ИИ в цифровом мире.

Что мы сделали

- Представили на Форуме ООН по управлению интернетом (IGF) 2024 года[1] в Эр-Рияде руководство по безопасной разработке и внедрению систем на основе ИИ (Guidelines for Secure Development and Deployment of AI Systems). Цель документа — помочь организациям избежать киберрисков, связанных с применением технологий ИИ.
- Подписали Пакт Европейской комиссии об искусственном интеллекте (AI Pact), подтвердив готовность выстраивать стратегию управления ИИ в логике будущего Закона об искусственном интеллекте ЕС (EU AI Act).
- Присоединились к Глобальному альянсу по ИИ для промышленности и производства, созданному в 2023 году ООН по промышленному развитию (ЮНИДО), и к Альянсу в сфере искусственного интеллекта (a-ai.ru), который объединяет ведущие российские технологические компании с целью ответственного развития ИИ.
- Сформулировали для стейкхолдеров понятные ориентиры в этой области: от моделирования угроз и оценки рисков до защиты от ИИ-атак и соблюдения международных норм (например, GDPR).
- Взяли на себя обязательства принять внутреннюю стратегию по управлению ИИ и повышать осведомленность сотрудников и других лиц в области взаимодействии с ИИ.
- Подтвердили наши принципы ответственного применения ИИ в кибербезопасности: прозрачность, безопасность, человеческий контроль, право на цифровую приватность, приверженность целям кибербезопасности и открытость к диалогу.

Что в результате

- Мы укрепили роль «Лаборатории Касперского» как одного из лидеров в формировании глобальных стандартов этичного ИИ в кибербезопасности.
- Стали активным участником общеевропейской дискуссии по регулированию ИИ и подготовили Компанию к требованиям EU AI Act.
- Донесли до партнеров, клиентов, регуляторов и профессионального сообщества, как мы обеспечиваем надежность и безопасность ИИ-систем, и пригласили их к выработке общих этических принципов цифрового развития.

Планы по развитию GTI на 2026–2027 годы

- Возможное расширение сети Центров прозрачности (Азиатско-Тихоокеанский регион)
- Диверсификация дата-центров, развитие инфраструктуры по обработке вредоносных и подозрительных файлов
- Продолжение практики приглашения стейкхолдеров в Центры прозрачности
- Ресертификация по ключевым стандартам
- Продолжение публикации отчетов о запросах данных

[1] Ежегодный международный Форум ООН по управлению интернетом, в 2024 году он прошел в Эр-Рияде с 15 по 19 декабря.

Устойчивая цепочка поставок

Закупочная деятельность «Лаборатории Касперского» строится на принципах прозрачности, добросовестной конкуренции и равных условий для всех потенциальных контрагентов.

Всем компаниям, заинтересованным в сотрудничестве, предоставляется равный доступ к участию в конкурсных процедурах.

Как мы организуем закупочную деятельность

Процессы закупок регламентируются внутренними документами «Лаборатории Касперского», включая закупочную политику и политику по контрактам. В 2025 году была принята обновленная закупочная политика, направленная на повышение эффективности и управляемости закупочной функции. Ключевые цели обновления включали:

- упрощение процедур — внедрение более понятных и детализированных правил, а также упрощение порядка проведения более 20% от общего объема закупок;
- снижение ключевых рисков — усиление контрольных механизмов и внедрение годового планирования;
- повышение осведомленности сотрудников — развитие обучающих материалов и тренингов, а также сокращение числа исключений из стандартных процедур.

Компания уделяет особое внимание соблюдению утвержденных правил как внутри организации, так и со стороны поставщиков. Принципы устойчивых закупок доводятся до сведения контрагентов через тендерную и договорную документацию.

В рамках цифровизации закупочной функции «Лаборатория Касперского» внедряет IT-решение для управления закупками, разработанное российским вендором.

Закупки в Компании организованы по категорийной модели. Категоризация основана на сходстве технических и функциональных характеристик, областях применения и бизнес-направлениях (маркетинг, профессиональные сервисы, IT, производственные затраты и др.). Для эффективного управления закупками установлены пороговые значения в зависимости от кумулятивного годового объема закупок по категориям:

- закупки до $25 000 проводятся по упрощенной процедуре с получением не менее двух конкурентных предложений;
- закупки в диапазоне от $25 000 до $100 000 требуют минимум трех предложений либо двух — от доверенных поставщиков, отобранных по итогам тендеров и имеющих успешный опыт работы с Компанией;
- закупки свыше $100 000 проводятся в форме тендера с участием отдела закупок, тендерного комитета и кросс-функциональных команд.

Для тендерных процедур также предусмотрены дополнительные уровни вовлеченности руководства в зависимости от бюджета. Так, при закупках на сумму около $1 млн в процессе участвует бизнес-директор «Лаборатории Касперского».

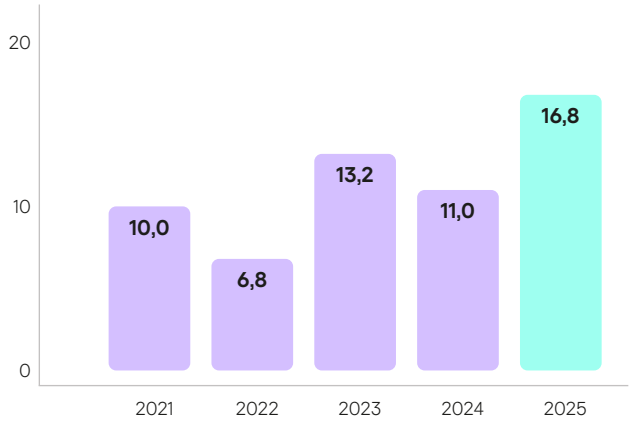
Перед приглашением партнера к участию в тендере наша служба безопасности проводит его проверку. Компания сотрудничает только с контрагентами, имеющими подтвержденный опыт и деловую репутацию: 99% наших поставщиков работают на рынке не менее трех лет. Все договоры содержат антикоррупционную оговорку.

GRI 2-6

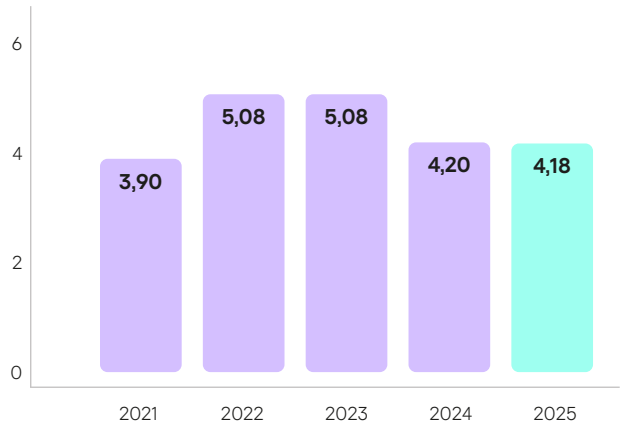
Закупки проводятся как напрямую у производителей (вендоров), так и через дистрибьюторов и партнерские сети — в зависимости от бизнес-модели поставщика и специфики региона.

В 2025 году количество поставщиков Компании сохраняется примерно на том же уровне, что в предыдущие годы. Экономия средств за счет конкурсных процедур и оптимизации издержек стабилизировалась и в среднем составила около 7% от объема закупок, охваченных закупочной функцией.

Экономия Компании в результате тендеров и сокращения издержек при закупке товаров и услуг[1], $ млн



Количество поставщиков Компании на конец отчетного периода, тысяч штук



GRI 204-1, СОКБ 65, СОКБ 66

В 2024 и 2025 годах около 50% общего объема закупок пришлось на российских поставщиков. При этом доля закупок у представителей малого и среднего бизнеса составила порядка 80% от общего объема закупок.

Планы на 2026 год

В 2026 году планируется дальнейшее развитие закупочной функции как бизнес-партнера: активное участие закупок в процессах планирования и бюджетирования, а также совместная с бизнес-подразделениями разработка и реализация дорожной карты закупочных проектов.

7%

средняя экономия средств при закупках за счет конкурсных процедур и сокращения издержек

>4 000 поставщиков

сотрудничали с Компанией в 2024–2025 годах

[1] Без учета затрат по третьим лицам.

Управление рисками

В нашей Компании внедрена и последовательно развивается система управления рисками, основанная на проактивном подходе и ориентированная на своевременное реагирование на внутренние и внешние вызовы.

СОКБ 53

«Лаборатория Касперского» стремится не только минимизировать последствия реализации рисков, но и предотвращать их возникновение на ранних этапах.

Принципы управления рисками разработаны с учетом требований законодательства Российской Федерации, нормативных актов Центрального Банка Российской Федерации и международных практик в области риск-менеджмента. При развитии системы Компания ориентируется на современные подходы и лучшие отраслевые стандарты в области управления рисками.

Развитие системы управления рисками

В 2024–2025 годах «Лаборатория Касперского» активно развивала систему управления рисками (СУР), сформированную на базе процесса Global Problem Management (GPM), изначально созданного для управления технологическими рисками. В процесс были вовлечены новые подразделения и дочерние компании, разработаны удобные дашборды для регулярного мониторинга рисков и инцидентов.

Цели и задачи управления рисками

Целями управления операционными рисками являются своевременное выявление рисков и снижение их влияния, позволяющие обеспечивать устойчивое функционирование и развитие бизнеса Компании, поддержание высокого качества ее продуктов и сервисов в условиях высокой турбулентности внешней среды.

В рамках процесса GPM Компания управляет технологическими рисками — своевременно выявляет их и ведет непрерывную работу по их снижению. Такой подход позволяет предотвращать инциденты, связанные с качеством продуктов и сервисов, а также с функционированием внутренней и внешней IT-инфраструктуры.

Ключевые задачи управления рисками:

1. идентификация рисков, способных существенно повлиять на Компанию или пользователей ее продуктов и сервисов;
2. анализ и оценка выявленных рисков;
3. разработка и реализация планов по минимизации рисков;
4. мониторинг и контроль как новых, так и ранее идентифицированных рисков, включая случаи, когда их полное устранение невозможно.

Принципы управления операционными рисками

Формирование рискориентированной среды

Управление рисками является неотъемлемой частью деятельности Компании и не ограничивается функциями отдельного подразделения. Процесс GPM обеспечивает работу с рисками как внутри отдельных департаментов, так и на пересечении зон ответственности нескольких подразделений. По мере развития СУР в процесс вовлекаются новые функции и команды.

Непрерывность и обязательность процесса управления рисками

Процесс управления рисками продолжается непрерывно. В подразделениях, вовлеченных в GPM, назначены сотрудники, для участия в выявлении, анализе, оценке рисков и разработке планов по их минимизации. Синхронизация по новым рискам и инцидентам проводится не реже одного раза в две недели, а актуализация статусов активных рисков — не реже одного раза в квартал.

Информирование руководителей на каждом уровне принятия решений

В Компании действует система коммуникаций и отчетности, позволяющая своевременно информировать руководителей всех уровней об актуальной карте рисков, связанных с принимаемыми ими решениями: активных, принятых и закрытых рисках. Это создает основу для рискориентированного принятия решений.

Открытость и единые методы оценки

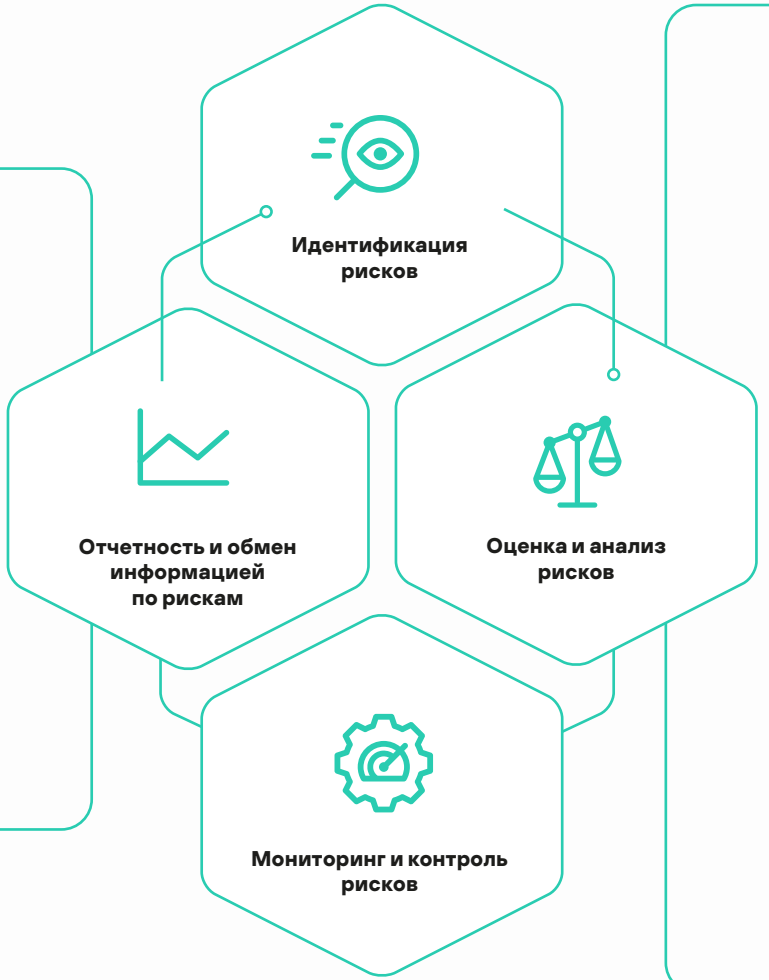
Для анализа рисков в Компании применяются единые классификаторы и шкалы оценки, закрепленные в документации по GPM и используемые всеми вовлеченными подразделениями. В случае разногласий или выявления недостатков методологии проводятся сессии фасилитации, по итогам которых классификаторы и методы оценки дорабатываются.

Процесс управления операционными рисками

Отчетность и обмен информацией о рисках

Чтобы способствовать принятию объективных и действенных управленческих решений, Компания внедрила многоступенчатую систему отчетности по рискам. В отчетах и дашбордах отражается динамика работы над рисками, изменение их значимости, статистика по принятым и закрытым рискам, а также выделяются наиболее критичные риски текущего периода.

Генеральный директор «Лаборатории Касперского» ежегодно получает отчет о наиболее значимых рисках и инцидентах. Ежеквартальная отчетность о рисках представляется управляющему совету. Кроме того, статус рисков и инцидентов регулярно обсуждается с руководителями департаментов, структурных подразделений и их сотрудниками.



Идентификация (выявление) рисков представляет собой многоплановый процесс, распределенный между различными подразделениями Компании. Риски выявляются на основе анализа произошедших инцидентов, моделирования потенциальных инцидентов и анализа бизнес-процессов. Выявленные риски анализируются и оцениваются согласно разработанным шкалам классификации, согласованным и утвержденным между всеми вовлеченными департаментами.

Каждый выявленный риск проходит **анализ и оценку** по двум ключевым параметрам: вероятности реализации и масштабу фактического или потенциального ущерба для Компании и ее клиентов. Для каждого риска определяется владелец, причины возникновения, возможные последствия, а также формируется план мероприятий по снижению риска с назначением ответственных лиц.

Мониторинг фактически понесенных и потенциальных потерь ведется Компанией на регулярной основе. Все инциденты фиксируются, проводится обязательная оценка ущерба, а также детальный анализ источников и причин рисков.

Контроль рисков в Компании носит непрерывный характер и направлен:

- на использование информации о рисках при принятии управленческих решений;
- регулярный контроль статусов активных рисков в соответствии с утвержденным процессом;
- своевременную реализацию эффективных мер по снижению рисков, способных повлиять на деятельность Компании.

Управление ESG-рисками

За управление рисками устойчивого развития в «Лаборатории Касперского» отвечают топ-менеджеры Компании и руководители направлений. В отчетном периоде Компания выделила два существенных[1] ESG-риска: риск изменений в политической и экономической обстановке в регионах присутствия, изменений в законодательстве и риск роста киберпреступности.

Ключевые ESG-риски

SASB TC-SI-550a.2

Риск изменений в политической и экономической обстановке в регионах присутствия Компании, изменения в законодательстве

Почему риск важен

Возможны изменения в законодательстве, способные существенно ограничить способность Компании вести бизнес в стране/регионе присутствия

Меры по управлению рисками в 2024 и 2025 годах

- Постоянный мониторинг изменений в законодательстве в странах/регионах присутствия с целью оперативного выявления потенциальных рисков
- Членство Компании и отдельных сотрудников в различных отраслевых организациях для участия в коммуникации с регулирующими органами
- Участие в публичных консультациях, проводимых органами государственной власти в странах/регионах присутствия, по проектам внесения изменений в действующее регулирование или введения нового с целью продвижения позиции Компании
- Дальнейшее развитие GTI с целью верификации надежности Компании и ее продуктов клиентами, партнерами, а также регуляторами

Риск роста киберпреступности

Почему риск важен

В нынешних условиях наблюдается снижение уровня сотрудничества между правоохранительными органами и частными компаниями в разных странах. Чтобы не допустить всплеска киберпреступности, важно сохранить сотрудничество и обмен экспертизой с частным сектором

Меры по управлению рисками в 2024 и 2025 годах

Компания продолжила активно сотрудничать с правоохранительными органами и международными организациями в отчетном периоде:

- внесла свой вклад в проведение ряда операций под эгидой Интерпола, в том числе Synergia и Synergia II, Serengeti и Serengeti 2.0, Red Card и Secure;
- помогла обеспечить безопасность крупных международных спортивных мероприятий, таких как летние Олимпийские игры 2024 года в Париже и Гран-при Сингапура в рамках чемпионата мира «Формулы-1» 2025 года;
- поделилась данными для двух изданий Interpol Africa Cyberthreat Assessment Report (2024, 2025), в которых представлен ландшафт киберугроз и атак на Африканском континенте;
- приняла участие в трех встречах экспертных рабочих групп под эгидой Интерпола, проходивших в Бангкоке, Ханое и Дохе, где поделились экспертизой в исследовании киберугроз с представителями правоохранительных органов, агентств по кибербезопасности, других государственных структур и частных компаний;
- участвовала в формировании отзывов и предложений к нескольким документам, разрабатываемым под эгидой ООН, включая Конвенцию против киберпреступности и Глобальный цифровой договор;
- подписала меморандумы о взаимопонимании с Африполом и рядом национальных регуляторов в области кибербезопасности.

Реализовавшиеся риски

SASB TC-SI-220a.5

В отчетном периоде были зафиксированы следующие риски, реализовавшиеся в условиях геополитической нестабильности:

- прекращение сотрудничества отдельных контрагентов с «Лабораторией Касперского»;
- сложности с оплатой товаров и услуг за рубежом.

В частности, 20 июня 2024 года министерство торговли США ввело запрет на продажу и использование в стране программного обеспечения «Лаборатории Касперского». В связи с этим Компания прекратила продажи ПО и начала сворачивать операционную деятельность в стране. «Лаборатория Касперского» считает, что такое решение было принято на фоне геополитической ситуации и не основано на технической оценке продуктов. При этом Компания сохраняет возможность продавать и продвигать на территории США сервисы информирования об угрозах Threat Intelligence[2], обучения по информационной безопасности (Kaspersky Threat Intelligence и Kaspersky Cybersecurity Training) и консалтинговые услуги (SOC Consulting, Security Consulting, Ask the Analyst и Incident Response).

Планы на 2026 год

В 2026 году «Лаборатория Касперского» планирует сосредоточиться на систематизации и агрегации накопленной базы рисков, а также на дальнейшей оптимизации форматов отчетности и аналитических инструментов.

[1] Существенные риски — это риски, которые, по мнению руководства Компании, могут оказать существенное влияние на результаты деятельности.

[2] Аналитика и мониторинг киберугроз — сбор, анализ и интерпретация данных о существующих и потенциальных кибератаках.

Дополнительная информация

Приложение 1. Об Отчете

GRI 2-1, GRI 2-2, GRI 2-3

В настоящем Отчете «Лаборатория Касперского» учитывает подходы и показатели, предусмотренные следующими международными и российскими стандартами в области устойчивого развития:

- Руководство Глобальной инициативы по отчетности (GRI 2021);
- отраслевое руководство Sustainability Accounting Standards Board (SASB) для сектора Software & IT Services;
- Стандарт общественного капитала бизнеса (СОКБ), утвержденный постановлением Правительства Российской Федерации от 30 декабря 2025 года № 2230.

Информация о соответствии раскрываемых сведений требованиям этих стандартов представлена в разделах «Указатель соответствия Руководству GRI Standards», «Указатель соответствия Руководству SASB Standards» и «Указатель соответствия СОКБ».

Если не указано иное, информация, представленная в Отчете, охватывает деятельность акционерного общества «Лаборатория Касперского» и компаний Kaspersky в странах присутствия (региональные офисы).

Отчет охватывает период с 1 января 2024 года по 31 декабря 2025 года.

Прогнозные заявления и планы «Лаборатории Касперского», отраженные в настоящем Отчете, носят предварительный характер. Они могут изменяться под влиянием внешних и внутренних факторов, которые на момент подготовки Отчета не могли быть в полной мере учтены. В связи с этим фактические результаты деятельности в области устойчивого развития в последующих отчетных периодах могут отличаться от представленных в настоящем Отчете.

Отчет опубликован на сайте Компании на русском и английском языках.

Приложение 2. Определение существенных тем

GRI 3-1, GRI 3-2

Чтобы содержание нашего Отчета в наибольшей мере отвечало интересам и ожиданиям заинтересованных сторон, мы провели опрос стейкхолдеров с целью определения существенных тем Отчета в форме онлайн-анкетирования. Анкетирование проводилось с 9 октября по 10 ноября 2025 года на русском и английском языках.

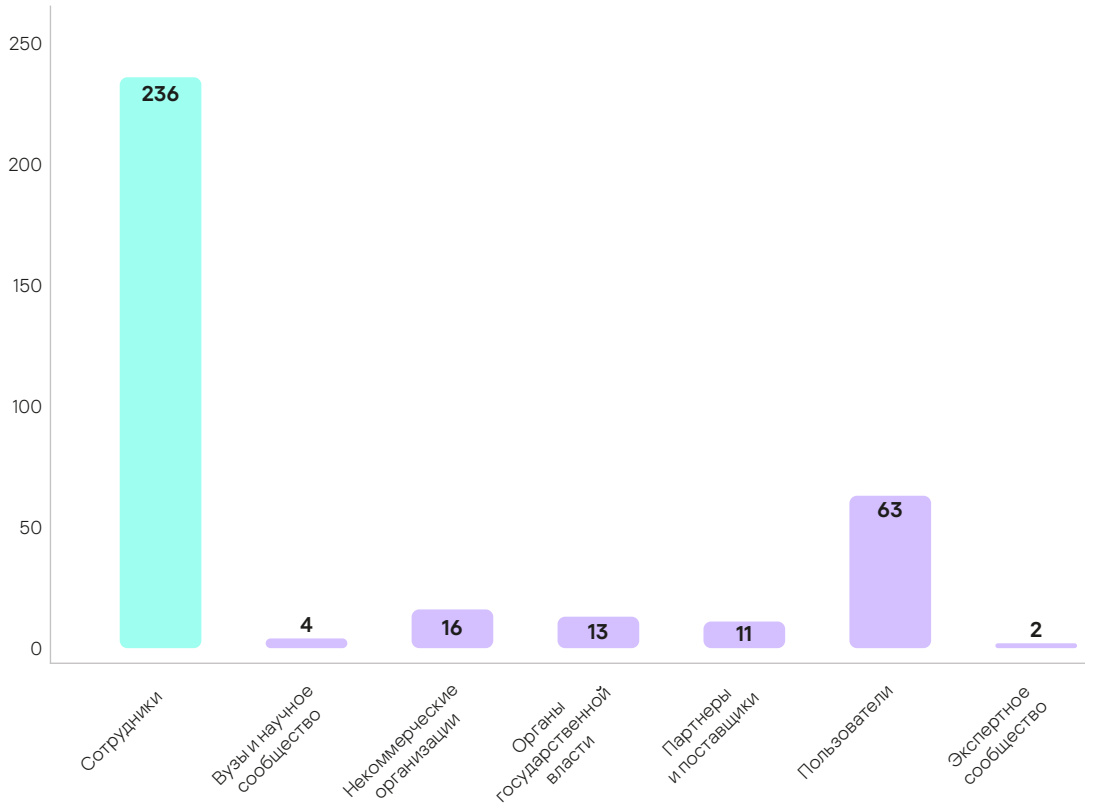
Первоначальный список тем Отчета для оценки стейкхолдерами был составлен на основе перечня приоритетных тем, сформированного в рамках процедуры определения существенности для предыдущего отчетного периода. Формулировки трех тем были уточнены внутренней экспертной группой Компании. Также ей были дополнены списки аспектов, которые отражает каждая тема.

Список включал 17 тем, которые отражают воздействия Компании на экономику, окружающую среду и общество. Участники анкетирования могли оценить значимость каждой из предложенных тем по шкале от 1 до 5 баллов, где 1 получали наименее важные, а 5 — исключительно важные темы. В анкете также была предусмотрена возможность оставлять замечания в свободной форме: стейкхолдеры могли как прокомментировать темы, предложенные для оценки, так и предложить новые. В опросе приняли участие 345 представителей заинтересованных сторон: 236 внутренних и 109 внешних стейкхолдеров.

Полученные результаты были скорректированы с помощью весовых коэффициентов, чтобы придать равную значимость мнению каждой из групп стейкхолдеров. Затем на основе усредненных оценок, полученных от заинтересованных сторон, был сформирован итоговый список тем в порядке убывания их значимости. Существенными для отражения в Отчете были признаны восемь тем, набравших общую оценку четыре балла и более. Это позволило в равной мере учесть мнения как внутренних, так и внешних стейкхолдеров, принимавших участие в опросе.

Формулировка из анкеты 2023 года	Формулировка из анкеты 2025 года
Защита пользователей и пользовательских данных	Защита данных
Просвещение в области информационной безопасности	Цифровое просвещение
Инклюзивная цифровая среда	Инклюзия

Участники анкетирования в разбивке по категориям стейкхолдеров, человек

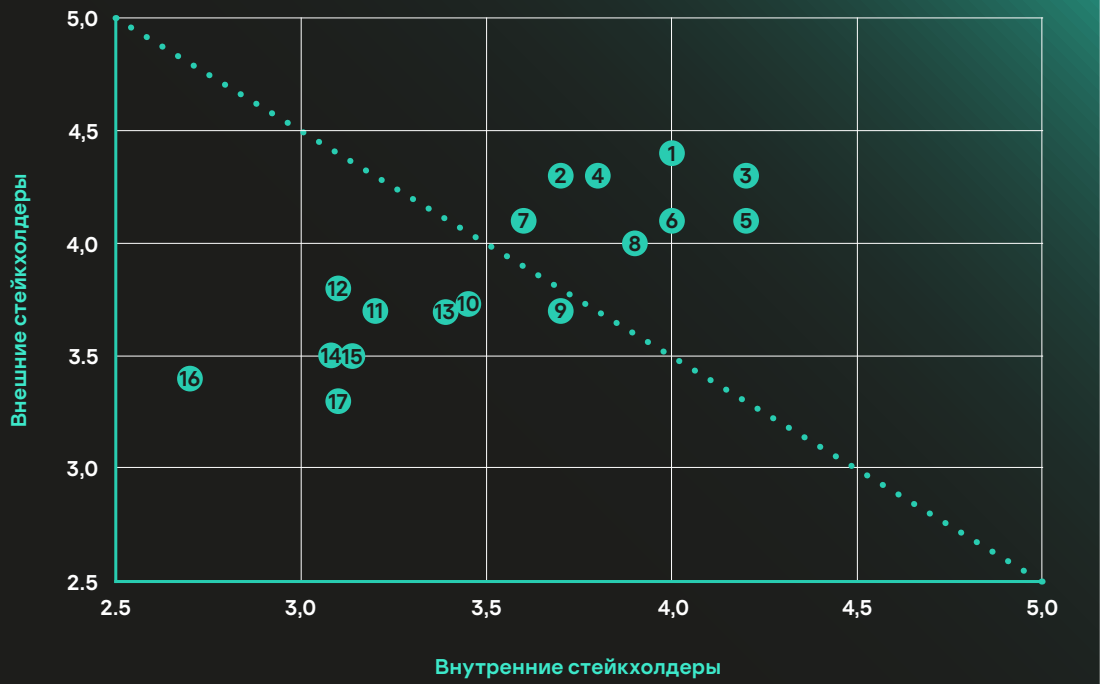


Список существенных тем «Лаборатории Касперского» в Отчете об устойчивом развитии за 2024—2025 годы

Тема	Оценка существенности	Страница отчета
Защита данных	4,3	109
Безопасная цифровая среда	4,2	45
Борьба с международной киберпреступностью	4,2	26
Подготовка профессионалов для отрасли	4,2	82
Ответственность перед сотрудниками	4,1	57
Обеспечение программно-цифровой устойчивости в меняющемся мире	4,1	49
Цифровое просвещение	4,1	87
Вклад в развитие технологий	4,0	24

Номер темы	Название темы
1	Защита данных
2	Безопасная цифровая среда
3	Борьба с международной киберпреступностью
4	Подготовка профессионалов для отрасли
5	Ответственность перед сотрудниками
6	Обеспечение программно-цифровой устойчивости в меняющемся мире
7	Цифровое просвещение
8	Вклад в развитие технологий
9	Прозрачность бизнеса и корпоративного управления
10	Деловая этика
11	Устойчивая цепочка поставок
12	Инклюзия

Оценка существенных тем внешними и внутренними стейкхолдерами



Номер темы	Название темы
13	Информационная и технологическая открытость
14	Социальные проекты, благотворительность и волонтерство
15	Женщины в STEM
16	Снижение климатического и экологического следа
17	Налогообложение

Приложение 3. Участие в ассоциациях и объединениях

GRI 2-28

«Лаборатория Касперского» сотрудничает и участвует в совместных инициативах со следующими организациями:

- Интерпол;
- Африпол;
- Альянс No More Ransom (совместно с Европолом) — за девять лет работы помог более 6 млн пользователей восстановить свои данные без выплаты выкупа;
- Коалиция против сталкерского 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 (ITU);
- Международная организация по стандартизации (ISO);
- Международный альянс Smart Africa.

Приложение 4. К разделу «Люди в «Лаборатории Касперского»

Среднесписочная численность сотрудников Компании, человек

СОКБ 25

2023[1]			2024			2025		
Женщины	Мужчины	Всего	Женщины	Мужчины	Всего	Женщины	Мужчины	Всего
1 301	3 727	5 028	1 290	3 794	5 084	1 329	4 025	5 354

Общая численность с разбивкой по типу трудового договора и по полу, человек

GRI 2-7

2023				2024				2025			
Постоянный		Временный		Постоянный		Временный		Постоянный		Временный	
Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины
1 257	3 770	45	47	1 254	3 748	34	43	1 352	4 186	39	55

Общая численность работников с разбивкой по типу занятости и по полу, человек

GRI 2-7

2023				2024				2025			
Полная		Частичная		Полная		Частичная		Полная		Частичная	
Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины	Женщины	Мужчины
1 265	3 796	37	21	1 253	3 764	35	27	1 365	4 215	26	26

[1] Показатель за 2023 год был скорректирован относительно ранее опубликованных данных в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Общая численность работников с разбивкой по возрасту

GRI 2–7, СОКБ 25

Возраст работников	2023		2024		2025	
	Человек	%	Человек	%	Человек	%
До 30 лет	1 161	23	1 100	22	1 298	23
От 30 до 50 лет	3 635	71	3 617	71	3 926	70
50 лет и старше	326	6	370	7	423	7

Общая численность в разбивке по регионам[1], человек

GRI 2–7

Регион	2023	2024	2025
Азиатско-Тихоокеанский регион	227	225	233
Латинская Америка	134	144	176
Ближний Восток, Турция и Африка	135	166	187
Европа	341	283	235
СНГ	4 250	4 290	4 858
■ В том числе Россия	4 221	4 261	4 827

[1] Здесь и далее из региональных разбивок исключены регионы, численность сотрудников в которых составляет менее 1% от общей численности, поскольку при малой базе раскрытие данных не является репрезентативным.

Структура персонала по категориям сотрудников

GRI 405-1, СОКБ 49

Возраст работников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Руководители	846	16	869	17	958	17	10
■ Из них мужчины	627	75	632	73	707	74	12
■ Из них женщины	211	25	232	27	246	26	6
■ Из них до 30 лет	45	5	42	5	43	5	2
■ Из них от 30 до 50 лет	698	83	717	83	789	83	10
■ Из них старше 50 лет	96	11	105	12	117	12	11
Технические специалисты	2 696	52	2 704	53	3 051	54	13
■ Из них мужчины	2 233	83	2 250	84	2 552	84	13
■ Из них женщины	447	17	443	16	487	16	10
■ Из них до 30 лет	786	30	752	28	914	31	22
■ Из них от 30 до 50 лет	1742	66	1 772	67	1 919	65	8
■ Из них старше 50 лет	95	4	116	4	140	5	21
Прочие специалисты	1 610	31	1 539	30	1 682	30	9
■ Из них мужчины	941	60	897	60	980	60	9
■ Из них женщины	638	40	607	40	654	40	8
■ Из них до 30 лет	292	19	271	18	314	19	16
■ Из них от 30 до 50 лет	1 140	73	1 068	72	1 148	71	7
■ Из них старше 50 лет	134	9	145	10	158	10	9

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Численность принятых работников, человек

GRI 401-1

2023	2024	2025	Изменение 2025/2024, %
944	563	961	71

Принятые работники с разбивкой по возрастным группам

Возраст сотрудников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
До 30 лет	312	38	201	37	408	44	103
От 30 до 50 лет	486	58	313	58	502	53	60
50 лет и старше	34	4	27	5	28	3	8

Принятые работники с разбивкой по полу

Пол сотрудников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Мужчины	703	76	390	71	732	77	86
Женщины	222	24	158	29	213	23	36

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с уточнением персональных данных работников.

Численность принятых работников по региону, человек

Регион	2023	2024	2025
Азиатско-Тихоокеанский регион	33	39	53
Латинская Америка	39	24	42
Ближний Восток, Турция и Африка	50	47	53
Европа	41	16	16
СНГ	778	436	796
■ В том числе Россия	769	432	790

Численность выбывших работников, человек

Показатель	2023[1]	2024	2025	Изменение 2025/2024, %
Выбывшие сотрудники	779	750	533	–30

Выбывшие работники с разбивкой по возрастным группам

Возраст работников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
До 30 лет	246	32	173	24	131	26	–24
От 30 до 50 лет	470	62	483	67	324	64	–33
50 лет и старше	48	6	64	9	54	11	–16

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Выбывшие работники с разбивкой по полу

Пол работников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Мужчины	521	67	519	70	361	68	–30
Женщины	253	33	220	30	168	32	–24

Численность выбывших работников по региону, человек

Регион	2023[1]	2024	2025
Азиатско-Тихоокеанский регион	30	49	40
Латинская Америка	13	16	16
Ближний Восток, Турция и Африка	20	19	36
Европа	54	78	57
СНГ	655	527	382
■ В том числе Россия	648	523	378

Текучесть персонала в разбивке по полу и возрасту, %

GRI 401-1, СОКБ 34

Показатель	2023	2024	2025	Изменение 2025/2024, %
Общая текучесть	15	15	10	–32
■ Текучесть среди мужчин	14	14	9	–38
■ Текучесть среди женщин	20	17	12	–29
■ Текучесть среди сотрудников младше 30 лет	22	16	10	–37
■ Текучесть среди сотрудников от 30 до 50 лет	13	14	8	–38
■ Текучесть среди сотрудников старше 50 лет	15	17	13	–26

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Текучесть персонала по региону, %

Регион	2023	2024	2025
Азиатско-Тихоокеанский регион	13	21	17
Латинская Америка	10	11	10
Ближний Восток, Турция и Африка	16	12	20
Европа	16	24	23
СНГ	16	12	8
■ В том числе Россия	16	12	8

Сотрудники, имевшие право на отпуск по уходу за ребенком

GRI 401-3

Пол работников	2023		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Женщины	1 296	25	1 282	25	1 387	25	8
Мужчины	3 801	75	3 779	75	4 239	75	12

Сотрудники, которые воспользовались правом на отпуск по уходу за ребенком

Пол работников	2023		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Женщины	55	93	44	98	42	95	–5
Мужчины	4	7	1	2	2	5	100

Сотрудники, которые вернулись после отпуска по уходу за ребенком

Пол работников	2023[1]		2024		2025		Изменение 2025/2024, %
	Человек	%	Человек	%	Человек	%	
Женщины	46	92	32	97	34	97	6
Мужчины	4	8	1	3	1	3	0

Коэффициент возвращения на работу сотрудников, %

Год	Женщины	Мужчины
2023[1]	98	100
2024	98	100
2025	100	100

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Коэффициент удержания сотрудников, %

Год	Женщины	Мужчины
2023[1]	73	50
2024	69	100
2025	67	100

Количество сотрудников, прошедших обучение по программам повышения квалификации и профессиональной подготовки, человек

Категория сотрудников	2024	2025
Общее количество сотрудников, прошедших обучение по программам повышения квалификации и профессиональной подготовки, в том числе:	203	222
■ Руководители	40	39
■ Технические специалисты	95	137
■ Прочие специалисты	108	85
■ Мужчины	129	158
■ Женщины	74	64

[1] Данные за 2023 год отличаются от данных, представленных в Отчете об устойчивом развитии за вторую половину 2022 года и 2023 год, в связи с переходом на новые источники данных, изменениями в персональных данных и учетом сотрудников, не попавших в прошлый Отчет.

Приложение 5. К разделу «Цифровая безопасность»

Список стандартов в области кибербезопасности, по которым сертифицированы решения KICS for Nodes и KICS for Network, входящие в платформу KICS, а также других международных законов и отраслевых стандартов, требования которых они учитывают или помогают исполнить:

- ISO/IEC 27001 IEC 27002 (DIN 2008 в Германии) — стандарт, устанавливающий требования к созданию, внедрению, поддержанию и постоянному совершенствованию системы управления информационной безопасностью в контексте организации;
- ISO/IEC 27019 (DIN 2011 в Германии) — стандарт, использующийся для обеспечения информационной безопасности в энергетике;
- ISO/IEC 27032 — стандарт, касающийся вопросов обеспечения безопасности в интернете и содержит рекомендации по устранению наиболее распространенных угроз в этой сфере (социальная инженерия, атаки нулевого дня, шпионское ПО и так далее);
- ISO/IEC 15408 — стандарт, который имеет исторически сложившееся название «Общие критерии» и представляет собой обобщенный опыт различных государств по разработке и практическому использованию критериев оценки безопасности информационных технологий;
- IEC 62443 (ANSI/ISA 99) — серия этих стандартов содержит требования к проектированию систем управления кибербезопасностью АСУ ТП и SCADA;
- NIST CSF — рекомендации по обеспечению безопасности промышленных систем управления, разработанные Национальным институтом стандартов и технологий США (NIST), поддерживается в том числе ONG-C2M2, API-1164, TSA PSF, CISA;
- NIST SP 800-82 — руководство США по защите промышленных систем управления (ICS), охватывает управление рисками, контроль доступа, реагирование на инциденты, мониторинг безопасности и др.;
- NERC CIP — свод стандартов кибербезопасности для критической инфраструктуры и защиты энергосистемы США, на которые также ориентируются некоторые страны Латинской Америки;
- NIS 2 Directive (EU) 2022/2555 — новая директива ЕС о кибербезопасности;
- NIS/NIS2 — первая общеевропейская директива по кибербезопасности, установившая более высокий и единый уровень безопасности сетевых и информационных систем в ЕС;
- IEC 62351 — стандарты по безопасности систем управления электроэнергетикой и сопутствующих коммуникаций; задают требования к безопасности, мерам защиты и коммуникационным сетям в энергетике;
- IMO MSC.428(98) — резолюция Комитета по безопасности на море, которая регулирует управление киберрисками в морской отрасли в рамках систем управления безопасностью;
- ICAO — стратегия кибербезопасности в авиации[1];
- IAEA Nuclear Security Series No. 17-T (Rev. 1) — методы обеспечения компьютерной безопасности для ядерных установок.

[1] FAA Advisory Circular 119-1 — Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).

Приложение 6. Указатель соответствия Руководству GRI Standards

«Лаборатория Касперского» подготовила Отчет с указанием стандартов GRI за период с 1 января 2024 года по 31 декабря 2025 года.

GRI 1.	Применение GRI 1: Принципы 2021 года
Применимые отраслевые стандарты GRI	Отсутствуют применимые отраслевые стандарты GRI

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
Общее раскрытие				
GRI 2-1	Информация об организации	Основное юридическое лицо в Российской Федерации — акционерное общество «Лаборатория Касперского». Штаб-квартира организации расположена по адресу: 125212, Россия, г. Москва, Ленинградское шоссе, д. 39а, стр. 2. Юридическая информация: https://www.kaspersky.ru/legal		7
GRI 2-2	Юридические лица, включенные в отчетность организации в области устойчивого развития		Приложение 1	123
			Приложение 10	156
GRI 2-3	Отчетный период, периодичность и контактное лицо	Дата публикации отчета: 23.06.2026	Приложение 1	123
				156
GRI 2-4	Пересмотр данных	Часть данных о персонале за 2023 год пересчитаны в связи с актуализацией персональных данных работников, переходом на новые системы учета и уточнением методик расчета. В каждом таком случае в тексте даны соответствующие примечания		
GRI 2-5	Внешнее заверение отчета	Внешнего заверения Отчета не проводилось		
GRI 2-6	Деятельность, цепочка создания стоимости и другие деловые отношения		О Компании	8, 9
			Ответственное ведение бизнеса	117
GRI 2-7	Сотрудники		Люди в «Лаборатории Касперского»	59
			Приложение 4	128
GRI 2-8	Сотрудники, которые не являются наемными работниками	Все сотрудники состоят в трудовых отношениях с «Лабораторией Касперского»		

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
GRI 2-9	Структура и состав управления		Управление устойчивым развитием	17
			Ответственное ведение бизнеса	105
GRI 2-10	Выдвижение и избрание высшего органа управления		Ответственное ведение бизнеса	105
GRI 2-11	Председатель высшего органа управления		Ответственное ведение бизнеса	105
GRI 2-12	Роль высшего органа управления в обеспечении контроля над управлением воздействиями		Управление устойчивым развитием	17
GRI 2-13	Делегирование ответственности по управлению воздействиями		Ответственное ведение бизнеса	105
GRI 2-14	Роль высшего органа управления в отчетности по устойчивому развитию	Информацию в Отчете об устойчивом развитии утверждают представители профильных департаментов, юридический отдел и отдел по связям с общественностью		
GRI 2-15	Конфликт интересов		Ответственное ведение бизнеса	107
GRI 2-16	Сообщение о важнейших проблемах	Оповещение совета директоров о важнейших проблемах осуществляется представителями профильных департаментов по электронной почте или в ходе экстренных очных встреч		
GRI 2-17	Коллективные знания высшего руководящего органа		Ответственное ведение бизнеса	105
GRI 2-18	Оценка деятельности высшего органа управления		Ответственное ведение бизнеса	105
GRI 2-19	Политика вознаграждения	На момент подготовки Отчета политика вознаграждения Компании не учитывала результативность управления воздействиями Компании на экономику, социальную сферу и окружающую среду		
GRI 2-20	Процесс определения вознаграждения	Информация не раскрывается в связи с ограничениями внутренней Политики конфиденциальности Компании		
GRI 2-21	Годовой общий коэффициент компенсации	Информация не раскрывается в связи с ограничениями внутренней Политики конфиденциальности Компании		
GRI 2-22	Заявление о стратегии устойчивого развития		Обращение генерального директора	3
GRI 2-23	Стратегические обязательства		Управление устойчивым развитием	17
			Ответственное ведение бизнеса	101
GRI 2-24	Внедрение стратегических обязательств		Управление устойчивым развитием	17
			Ответственное ведение бизнеса	101, 106
GRI 2-25	Процессы устранения негативных воздействий		Управление устойчивым развитием	18
			Ответственное ведение бизнеса	106, 108
GRI 2-26	Механизмы для получения консультаций и выражения озабоченности		Ответственное ведение бизнеса	106

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
GRI 2-27	Соблюдение законов и нормативных актов	В отчетном периоде в «Лаборатории Касперского» не было выявлено случаев несоблюдения законодательства и нормативных требований; на Компанию не налагались штрафы или иные виды ответственности за нарушение законодательства		
GRI 2-28	Членство в ассоциациях		Приложение 3	126
GRI 2-29	Подход к взаимодействию с заинтересованными сторонами		Управление устойчивым развитием	21
GRI 2-30	Коллективные договоры	В «Лаборатории Касперского» коллективный договор отсутствует		
Существенные темы				
GRI 3-1	Процесс определения существенных тем		Приложение 3	124
GRI 3-2	Список существенных тем		Приложение 3	125
Экономическая эффективность				
GRI 201-1	Созданная и распределенная прямая экономическая стоимость		О Компании	15
Рыночное присутствие				
GRI 202-2	Доля топ-менеджмента из местных сообществ		Доля высшего руководства, принятого из числа местного населения, — 100%	
Непрямые экономические воздействия				
GRI 203-1	Инвестиции в инфраструктуру и безвозмездные услуги		Управление устойчивым развитием	18
			Вклад в развитие общества	74
GRI 203-2	Существенное непрямое экономическое воздействие		Управление устойчивым развитием	18
			Вклад в развитие общества	74
Практики закупок				
GRI 204-1	Доля расходов на местных поставщиков		Ответственное ведение бизнеса	118
Противодействие коррупции				
GRI 205-1	Деятельность организации, прошедшая оценку рисков, связанных с коррупцией		Ответственное ведение бизнеса	106
GRI 205-2	Информирование о политике и методах противодействия коррупции и обучение им		Ответственное ведение бизнеса	107
GRI 205-3	Подтвержденные случаи коррупции и предпринятые меры		Ответственное ведение бизнеса	107
Энергия				
GRI 302-1	Потребление энергии внутри организации		Окружающая среда	92
GRI 302-4	Сокращение потребления энергии		Окружающая среда	93

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
Водные ресурсы				
GRI 303-1	Ответственное управление водными ресурсами как ресурсами общего пользования		Окружающая среда	94
GRI 303-2	Управление воздействиями, связанными со сбросами воды	В Компании нет утвержденных нормативов качества сточных вод, так как сброс воды в природные водоемы не осуществляется	Окружающая среда	94
GRI 303-3	Водозабор		Окружающая среда	94
Выбросы				
GRI 305-1	Прямые выбросы парниковых газов (область охвата 1)	Методика сбора данных и расчета общего количества прямых выбросов парниковых газов по всем объектам Компании (область охвата 1) в процессе разработки, данные будут представлены в последующих отчетах		
GRI 305-2	Косвенные энергетические выбросы парниковых газов (область охвата 2)	Методика сбора данных и расчета общего количества косвенных выбросов парниковых газов от энергопотребления (область охвата 2) в процессе разработки, данные будут представлены в последующих отчетах		
GRI 305-3	Косвенные неэнергетические выбросы парниковых газов (область охвата 3)		Окружающая среда	91
GRI 305-5	Сокращение выбросов парниковых газов		Окружающая среда	91
GRI 305-6	Выбросы озоноразрушающих веществ	Компания не производит выбросы озоноразрушающих веществ		
GRI 305-7	Выбросы в атмосферу NO_x, SO_x и других значимых загрязняющих веществ	Компания не производит выбросы указанных загрязняющих веществ в атмосферу		
Отходы				
GRI 306-1	Образование отходов и связанные с ними существенные воздействия		Окружающая среда	95
GRI 306-2	Управление существенными воздействиями, связанными с отходами		Окружающая среда	95
GRI 306-3	Образование отходов		Окружающая среда	95
GRI 306-4	Утилизация отходов		Окружающая среда	95
GRI 306-5	Удаление и захоронение отходов		Окружающая среда	95
Занятость				
GRI 401-1	Число новых работников и текучесть кадров		Люди в «Лаборатории Касперского» Приложение 4	59 130

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
GRI 401-2	Льготы, предоставляемые сотрудникам, работающим на условиях полной занятости, которые не предоставляются сотрудникам, работающим на условиях временной или неполной занятости		Люди в «Лаборатории Касперского»	61
GRI 401-3	Отпуск по уходу за ребенком		Приложение 4	133
Здоровье и безопасность на рабочем месте				
GRI 403-1	Система управления вопросами охраны труда и промышленной безопасностью	Система менеджмента охраны труда и здоровья во всех офисах «Лаборатории Касперского» в границах раскрытия в Отчете соответствует требованиям действующего трудового законодательства на территориях присутствия Компании. Она включает в себя регулярные инструктажи сотрудников и проведение регулярной специальной оценки рабочих мест во всех подразделениях, систему управления рисками и расследования несчастных случаев, а также организацию мероприятий по улучшению условий труда. Ключевым показателем эффективности является отсутствие травм на рабочем месте	Люди в «Лаборатории Касперского»	71
GRI 403-2	Выявление опасностей, оценка рисков и расследование происшествий		Люди в «Лаборатории Касперского»	71, 72
GRI 403-4	Вовлечение работников, консультации и коммуникации по вопросам охраны труда и промышленной безопасности		Люди в «Лаборатории Касперского»	72
GRI 403-5	Обучение работников, связанное с вопросами охраны труда и безопасности на рабочем месте		Люди в «Лаборатории Касперского»	71
GRI 403-6	Профилактика и охрана здоровья работников		Люди в «Лаборатории Касперского»	72
GRI 403-8	Работники, охваченные системой управления вопросами охраны труда и промышленной безопасности	Все сотрудники Компании охвачены системой управления вопросами охраны труда		
GRI 403-9	Производственный травматизм		Люди в «Лаборатории Касперского»	71
GRI 403-10	Профессиональные заболевания	В отчетном периоде в АО «Лаборатория Касперского» не зафиксировано случаев профессиональных заболеваний		
Обучение и образование				
GRI 404-1	Среднегодовое количество часов обучения на одного работника		Люди в «Лаборатории Касперского»	68
GRI 404-2	Программы повышения квалификации работников и поддержки карьерных изменений		Люди в «Лаборатории Касперского»	69
GRI 404-3	Доля сотрудников, для которых проводятся периодические оценки результативности и развития карьеры		Люди в «Лаборатории Касперского»	70
Разнообразие и равные возможности				
GRI 405-1	Разнообразие состава органов управления и структуры персонала		Люди в «Лаборатории Касперского» Приложение 4	64 129

Индикатор	Название раскрытия	Комментарий	Раздел Отчета	Стр.
GRI 405-2	Соотношение базовой заработной платы и вознаграждений у мужчин и женщин		Люди в «Лаборатории Касперского»	64
Недопущение дискриминации				
GRI 406-1	Случаи дискриминации и принятые меры	В отчетном периоде случаев дискриминации не выявлено	Ответственное ведение бизнеса	101
Детский труд				
GRI 408-1	Операции и поставщики, подверженные значительному риску случаев детского труда	Компания не использует детский труд. У Компании также отсутствуют поставщики, подверженные риску использования детского труда		
Принудительный или рабский труд				
GRI 409-1	Операции и поставщики, подверженные значительному риску случаев принудительного или рабского труда	Компания не использует принудительный и рабский труд. У Компании также отсутствуют поставщики, подверженные риску использования принудительного труда		
Местные сообщества				
GRI 413-1	Подразделения с реализованными программами взаимодействия с местными сообществами, программами оценки воздействия деятельности на местные сообщества и программами развития местных сообществ	В отчетном периоде программы взаимодействия с местными сообществами реализовывались Компанией в России, Испании, Италии, Японии, Индии, ЮАР, Сингапуре, Малайзии	Возможности для людей	77
Защита данных клиентов				
GRI 418-1	Обоснованные жалобы и выявленные утечки персональных данных клиентов		Ответственное ведение бизнеса	109

Приложение 7. Указатель соответствия Руководству SASB Standards

Настоящий отчет подготовлен в соответствии с отраслевым стандартом SASB Software and IT Services, версия 2018-10 (TC-SI). Ниже приведена таблица соответствия.

Индикатор	Информация к раскрытию	Раздел отчета	Примечания	Стр.
Экологический след инфраструктуры				
TC-SI-130-a.1	1) Общее потребление энергии, 2) процент сетевой электроэнергии, 3) процент возобновляемой энергии	Окружающая среда		92
TC-SI-130-a.2	1) Общий водозабор, 2) общее потребление воды и процент каждого показателя в регионах водного стресса или с резким дефицитом воды	Окружающая среда	Данные о водозаборе приведены только для московского офиса АО «Лаборатория Касперского»	94
TC-SI-130-a.3	Учет экологических аспектов при стратегическом планировании потребностей дата-центров	Окружающая среда		93
Конфиденциальность персональных данных и свобода самовыражения				
TC-SI-220-a.1	Описание политик и практик, касающихся таргетированной рекламы и конфиденциальности персональных данных пользователей	Ответственное ведение бизнеса		109, 110
TC-SI-220-a.2	Количество пользователей, информация о которых используется во вторичных целях		Таких пользователей — 0 (ноль)	
TC-SI-220-a.3	Общая сумма денежных убытков, возникших в результате судебных разбирательств, связанных с нарушением конфиденциальности пользователей/клиентов	Ответственное ведение бизнеса		110
TC-SI-220-a.4	1) Число запросов государственных органов на получение информации о пользователях, 2) число пользователей, информация о которых была запрошена, 3) процент пользователей, информация о которых была раскрыта		1) Подробную информацию о запросах государственных органов можно найти в регулярном отчете «Лаборатории Касперского» Law Enforcement & Government Requests Report по ссылке. Последний отчет был опубликован за второе полугодие 2025 года. 2) Статистика не ведется. Мы учитываем только количество запросов от государственных органов. 3) 0% — «Лаборатория Касперского» пока не предоставляла такие данные государственным органам	
TC-SI-220-a.5	Список стран, в которых основные продукты или услуги подлежат государственному мониторингу, блокировке, фильтрации контента или цензуре	Ответственное ведение бизнеса		121
Безопасность данных				
TC-SI-230-a.1	1) Число утечек данных, 2) процент утечек, касающихся персональных данных пользователей, 3) число пострадавших пользователей	Ответственное ведение бизнеса		110

Индикатор	Информация к раскрытию	Раздел отчета	Примечания	Стр.
TC-SI-230-a.2	Описание подхода к выявлению и устранению рисков безопасности данных, включая использование сторонних стандартов кибербезопасности	Ответственное ведение бизнеса		109
Наем и управление квалифицированными кадрами со всего мира и их социокультурное разнообразие				
TC-SI-330-a.1	Доля сотрудников, которые 1) являются иностранными гражданами, 2) работают из-за границы		1) В АО «Лаборатория Касперского» на 31 декабря 2025 года работали 63 иностранных гражданина, что составляет 1,3% от общего количества сотрудников. По другим региональным офисам информация в отчетном периоде не собиралась. 2) АО «Лаборатория Касперского» неприменимо, так как российское трудовое законодательство не подразумевает работу за пределами Российской Федерации. По офисам вне России информация в отчетном периоде не собиралась	
TC-SI-330-a.2	Вовлеченность сотрудников	Люди в «Лаборатории Касперского»		70
TC-SI-330-a.3	Процент представленности обоих полов и расовых/этнических групп 1) среди руководства, 2) среди технического персонала, 3) среди всех остальных сотрудников	Люди в «Лаборатории Касперского» Приложение 4	Компания не ведет сбор информации по принадлежности сотрудников к этническим и расовым группам	64 129
Защита интеллектуальной собственности и конкурентное поведение				
TC-SI-520-a.1	Общая сумма денежных убытков, возникших в результате судебных разбирательств, связанных с защитой интеллектуальной собственности и недобросовестной конкуренцией	Ответственное ведение бизнеса		111
Управление системными рисками технологических сбоев				
TC-SI-550-a.1	Количество 1) проблем с производительностью, 2) перебоев в обслуживании, 3) общее время простоя для клиентов		Информация не раскрывается в связи с ограничениями внутренней политики конфиденциальности Компании	
TC-SI-550-a.2	Описание рисков, связанных с обеспечением бесперебойной работы систем	Ответственное ведение бизнеса		121
Показатели деятельности организации				
TC-SI-000.A	1) Количество лицензий или подписок, 2) процент облачных технологий		1) 813 2) 30%	
TC-SI-000.B	1) Возможности обработки данных, 2) доля аутсорсинга		1) 292 узла в локальной сети и 8 198 узлов на аутсорсинге 2) 96% аутсорсинга (коллокация)	
TC-SI-000.C	1) Объем хранилища данных, 2) доля аутсорсинга		1) Не менее 100 ПБ 2) Более 93% аутсорсинга (коллокация)	

Приложение 8. Указатель соответствия СОКБ

Настоящий Отчет подготовлен с учетом Стандарта общественного капитала бизнеса, утвержденного постановлением Правительства Российской Федерации от 30 декабря 2025 года № 2230. Ниже приведена таблица соответствия.

Некоторые показатели не раскрываются в связи с конфиденциальностью данных, неприменимостью к деятельности «Лаборатории Касперского», или отсутствием соответствующего учета. Компания работает над совершенствованием системы учета для более полного раскрытия в следующих отчетных периодах.

№	Показатель	Раздел отчета	Стр.	Примечания
Экологические показатели				
1	Общий объем забираемой воды	Окружающая среда	94	
2	Объем использованной воды из всех источников водоснабжения			Учет не ведется. Компания не использует воду для производственных нужд
3	Доля оборотного и повторно-последовательного водоснабжения в общем объеме собственного потребления воды из всех источников			Потребление воды в Компании ограничено хозяйственно-бытовыми нуждами в офисах и дата-центрах. Системы оборотного водоснабжения не используются
4	Объем сбросов сточных вод (загрязненных, нормативно-чистых, нормативно-очищенных) в водные объекты и загрязненных стоков, переданных на очистку другим предприятиям			Учет не ведется. Компания не использует воду для производственных нужд. Для отведения сточных вод из офисов и дата-центров используются общая канализационная система
5	Образовано отходов I–V классов опасности, всего, ■ Образовано отходов I класса ■ Образовано отходов II класса ■ Образовано отходов III класса ■ Образовано отходов IV класса ■ Образовано отходов V класса	Окружающая среда	95	
6	Обращение с отходами, всего ■ утилизировано отходов (в том числе для повторного применения, для энергетической утилизации) ■ обезврежено отходов ■ захоронено отходов	Окружающая среда	95	
7	Масса выбросов загрязняющих веществ в атмосферный воздух от стационарных источников			Компания не производит выбросов загрязняющих веществ в атмосферу
8	Масса выбросов парниковых газов, включая прямые и косвенные выбросы	Окружающая среда	91	На данный момент Компания оценивает только выбросы от деловых поездок сотрудников, которые относятся к косвенным неэнергетическим выбросам
9	Углеродный след продукции			Учет не ведется

№	Показатель	Раздел отчета	Стр.	Примечания
10	Расходы на реализацию мероприятий, связанных с охраной окружающей среды, всего ■ на охрану атмосферного воздуха и предотвращение изменения климата ■ на сбор и очистку сточных вод ■ на обращение с отходами ■ на сохранение биоразнообразия и природных территорий ■ на охрану и рациональное использование земель ■ на реабилитацию земель ■ на защиту окружающей среды от шумового, вибрационного и других видов физического воздействия ■ на обеспечение радиационной безопасности окружающей среды ■ на другие направления деятельности в сфере охраны окружающей среды	Окружающая среда	90	
11	Объем потребления возобновляемой и низкоуглеродной энергии			Учет не ведется
12	Собственное энергопотребление без учета отпуска тепла и электроэнергии внешним потребителям, всего, ■ электроэнергия ■ тепловая энергия ■ по видам использованного топлива	Окружающая среда	92	
13	Доля использованных вторичных ресурсов в общем объеме использования материальных ресурсов для производства товаров, выполнения работ, оказания услуг или получения энергии			Учет не ведется
14	Плата за негативное воздействие на окружающую среду			В отчетном периоде Компания не осуществляла платежи за негативное воздействие на окружающую среду
15	Затраты на компенсации и штрафы в части: ■ штрафов за нарушения природоохранного законодательства; ■ компенсации вреда (ущерба), причиненного окружающей среде	Окружающая среда	90	
16	Аварии и инциденты, повлекшие за собой негативное воздействие на окружающую среду (в том числе в результате чрезвычайных ситуаций техногенного характера)			В отчетном периоде таких инцидентов с участием Компании не зафиксировано
17	Инвестиции в основной капитал, направленные на охрану окружающей среды и рациональное использование природных ресурсов, ■ на обращение со сточными водами ■ на охрану атмосферного воздуха и предотвращение изменения климата ■ на защиту и экологическую реабилитацию земель, поверхностных и подземных водных объектов ■ на обращение с отходами ■ на снижение шумового и вибрационного воздействия ■ на сохранение биоразнообразия и охрану природных территорий ■ на другие направления деятельности в области охраны окружающей среды			Учет не ведется
18	Наличие у организации сертификации системы энергетического менеджмента	Окружающая среда	92	

№	Показатель	Раздел отчета	Стр.	Примечания
Социальные показатели				
19	Расходы на оплату труда, всего			Информация не раскрывается в связи с политикой конфиденциальности Компании
20	Отношение средней заработной платы в организации к среднему уровню заработной платы в регионе			Учет не ведется
21	Среднесписочная численность работников	Люди в «Лаборатории Касперского»	59	
22	Расходы на реинтеграцию (профессиональную реабилитацию) работников, получивших статус инвалидов			В Компании отсутствуют программы по данному направлению
23	Доля работников-инвалидов			Учет не ведется
24	Доля работников, относящихся в соответствии с Федеральным законом «О ветеранах» к следующим категориям ветеранов: ■ ветераны Великой Отечественной войны; ■ ветераны боевых действий на территории СССР, на территории Российской Федерации и территориях других государств; ■ ветераны военной службы			Учет не ведется
25	Доля работников с указанием распределения по каждой из следующих категорий: пол; возрастная группа ■ Доля сотрудников-мужчин ■ Доля сотрудников-женщин ■ Доля сотрудников до 30 лет ■ Доля сотрудников 30—50 лет ■ Доля сотрудников старше 50 лет	Приложение 4	127	
26	Средняя заработная плата ■ по группам занятий (отдельно по руководителям и отдельно по иному персоналу) ■ по полу с учетом групп занятий ■ по возрастным группам			Информация не раскрывается в связи с политикой конфиденциальности Компании
27	Расходы на мероприятия по охране труда и промышленную безопасность, всего, ■ в том числе в среднем на одного работника			Учет не ведется
28	Расходы на организацию и проведение социальных, в том числе спортивных мероприятий для работников и членов их семей, всего, ■ в том числе в среднем на одного работника			Учет не ведется
29	Коэффициент частоты производственного травматизма персонала организации без учета персонала подрядчиков (LTIFR) на 1 000 000 человеко-часов	Люди в «Лаборатории Касперского»	71	В отчетном периоде в Компании не зафиксировано случаев производственного травматизма
30	Количество смертельных случаев работников организации без учета персонала подрядчиков			В отчетном периоде в Компании не зафиксировано смертельных случаев на производстве
31	Расходы организации на обучение работников, всего ■ на одного работника	Люди в «Лаборатории Касперского»	68	

№	Показатель	Раздел отчета	Стр.	Примечания
32	Среднее количество часов обучения в год на одного работника	Люди в «Лаборатории Касперского»	68	
33	Доля работников, охваченных коллективным договором, к среднесписочной численности работников			В Компании коллективный договор отсутствует
34	Коэффициент текучести кадров	Люди в «Лаборатории Касперского»	59	
		Приложение 4	132	
35	Расходы на участие в поддержке социальных программ, в том числе благотворительных программ, не направленных на работников и членов их семей, всего, в том числе в сфере: ■ здравоохранения; ■ образования и науки; ■ спорта; ■ культуры, искусства и туризма; ■ создания доступной инфраструктуры и инклюзивной среды; ■ благоустройства и развития комфортной городской среды; ■ создания и размещения социальной рекламы; ■ обеспечения жильем; ■ обеспечения общественной безопасности и антитеррористической защищенности объектов инфраструктуры; ■ поддержки граждан, нуждающихся в социальной помощи	Вклад в развитие общества	75	
36	Расходы на организацию и проведение медицинских мероприятий для работников и членов их семей, всего, ■ в том числе в среднем на одного работника			Учет не ведется
37	Доля работников, принимающих участие в проектах корпоративного добровольчества (волонтерства) и общее количество проектов корпоративного добровольчества (волонтерства)	Вклад в развитие общества	77	Около 400 сотрудников вовлечены в волонтерскую деятельность в Компании, что равно примерно 7% от общей численности. В Компании действует программа корпоративного волонтерства, которая включает семь направлений (донорство крови, спорт во благо, интеллектуальное волонтерство, помощь НКО в проведении мероприятий, проведение субботников в хосписах, поездки к подопечным в Удомельский детский дом, волонтерство в приютах для бездомных животных). В 2025 году сотрудники Компании участвовали более чем в 10 проектах в рамках направлений корпоративной программы волонтерства
38	Наложенные на организацию штрафы и меры ответственности в связи с нарушением трудового законодательства			Случаев нарушения трудового законодательства в отчетном периоде не зафиксировано
39	Среднее число детей в возрасте до шести лет на одного сотрудника			Учет не ведется
40	Среднее число детей на одного работника			Учет не ведется
41	Доля многодетных родителей от общего числа сотрудников			Учет не ведется
42	Доля работников, состоящих в зарегистрированном браке			Учет не ведется

№	Показатель	Раздел отчета	Стр.	Примечания
43	Размер единовременной выплаты (в том числе в виде материальной помощи), осуществляемой работникам при рождении ребенка, выплачиваемой в течение первого года после рождения ребенка	Люди в «Лаборатории Касперского»	65	
44	Наличие у организации системы менеджмента безопасности труда и охраны здоровья			Безопасность труда в «Лаборатории Касперского» обеспечивает департамент по работе с персоналом с привлечением внешних консультантов. В состав департамента входит Группа кадрового администрирования, отвечающая за охрану труда в Компании и здоровье сотрудников. Кроме того, в Компании действует комиссия по охране труда, в состав которой входят представители различных департаментов. Система менеджмента охраны труда включает в себя регулярные инструктажи сотрудников и проведение регулярной специальной оценки рабочих мест во всех подразделениях, систему управления рисками и расследования несчастных случаев, а также организацию мероприятий по улучшению условий труда
Управленческие показатели				
45	Наличие политики по устойчивому развитию и (или) иных стратегических документов в этой сфере (стратегия в области устойчивого развития, экологическая стратегия, стратегия реализации оперативных и долгосрочных мер по адаптации к изменениям климата и смягчению антропогенного воздействия на климат — климатическая стратегия)	Управление устойчивым развитием	17	
46	Наличие органа управления или комитета, созданных при коллегиальном органе управления организации, ответственных за утверждение и контроль реализации политики по устойчивому развитию и (или) иных стратегических документов в этой сфере (например, стратегии в области устойчивого развития, климатической стратегии)			Соответствующий орган управления в Компании отсутствует
47	Отражение в политике вознаграждения организации учета целевых показателей, связанных с устойчивым развитием и климатом, в целях определения размера вознаграждения ее руководящего состава			Показатели, связанные с устойчивым развитием и климатом, не влияют на размер вознаграждения руководящего состава Компании
48	Доля независимых директоров в составе коллегиального органа управления,	Ответственное ведение бизнеса	105	
49	Доля женщин-руководителей в общей численности руководителей, всего, ■ в том числе в коллегиальных органах управления	Приложение 4	129	Доля женщин в коллегиальных органах управления не раскрывается в связи с политикой конфиденциальности Компании
50	Количество зафиксированных случаев нарушения прав коренных малочисленных народов Российской Федерации			В отчетном периоде таких случаев не зафиксировано
51	Доля работников, замещающих должности с высоким коррупционным риском			Учет не ведется
52	Среднее количество часов обучения по вопросам противодействия коррупции на одного работника			Учет не ведется
53	Наличие политики по управлению рисками, в том числе климатическими, и (или) иных документов по управлению рисками	Ответственное ведение бизнеса	119	
54	Количество случаев привлечения к ответственности в соответствии с законодательством Российской Федерации за нарушение прав потребителей			В отчетном периоде случаев нарушения прав потребителей не зафиксировано

№	Показатель	Раздел отчета	Стр.	Примечания
55	Количество зафиксированных социально значимых инцидентов (забастовок)			В отчетном периоде таких инцидентов не зафиксировано
56	Наличие политики и (или) иных документов, предусматривающих применение принципов инклюзии в деятельности организации	Люди в «Лаборатории Касперского»	62	
57	Наличие у организации письменно зафиксированных обязательств комплексно осуществить деятельность в сфере инклюзии: ■ обеспечение доступности собственных территорий, помещений и услуг для людей с инвалидностью; ■ проведение просветительских и образовательных программ для персонала в сфере инклюзии; ■ внедрение технических решений для обеспечения доступности рабочих мест для людей с инвалидностью и создание рабочих мест для людей с инвалидностью с представлением ежеквартальной отчетности по исполнению указанных обязательств			С 2024 года в Компании проводятся аудиты доступности офисов для людей с инвалидностью с привлечением внешнего эксперта – РООИ «Перспектива». Результаты и рекомендации по итогам аудитов направляются в отделы, ответственные за управление офисом, безопасность, охрану, и управление персоналом
58	Сумма заявленных требований по судебным спорам с участием эмитента в качестве ответчика: ■ по делам о предъявлении требований к действующему или бывшему членам органов управления эмитента; ■ по делам об оспаривании сделок по статьям 173.1 и 174 Гражданского кодекса Российской Федерации; ■ по делам об оспаривании решений органов управления эмитента, а также споров с участием эмитента в иных судебных делах, связанных с нарушением корпоративного законодательства			Неприменимо
59	Сумма удовлетворенных требований по судебным спорам с участием эмитента в качестве ответчика			Неприменимо
60	Сумма штрафов, наложенных на организацию и должностных лиц в связи с нарушением требований законодательства Российской Федерации об акционерных обществах и ценных бумагах, в сфере корпоративных отношений в акционерных обществах			Неприменимо
Экономические показатели				
61	Выручка (показатель, аналогичный выручке)	О Компании	15	
62	Производительность труда	Люди в «Лаборатории Касперского»	70	
63	Сумма начисленных обязательных платежей (за исключением штрафов, пеней), всего в том числе: ■ налогов и сборов ■ страховых взносов ■ иных обязательных платежей			Информация не раскрывается в связи с политикой конфиденциальности Компании
64	Сумма уплаченных обязательных платежей (за исключением штрафов, пеней), всего, в том числе: ■ налогов и сборов; ■ страховых взносов; ■ иных обязательных платежей			Информация не раскрывается в связи с политикой конфиденциальности Компании
65	Доля закупок российских товаров, работ, услуг в общем объеме закупок товаров, работ, услуг	Ответственное ведение бизнеса	118	

№	Показатель	Раздел отчета	Стр.	Примечания
66	Доля закупок товаров, работ, услуг у субъектов малого и среднего предпринимательства в общем объеме закупок у российских организаций	Ответственное ведение бизнеса	118	
67	Объем устойчивых, в том числе зеленых, инвестиций и доля таких инвестиций в общем объеме инвестиций Доля устойчивых, в том числе зеленых, инвестиций в общем объеме инвестиций			Учет не ведется
68	Объем инвестиций в проекты, связанные с достижением технологического суверенитета и структурной адаптацией экономики Российской Федерации Доля инвестиций в проекты, связанные с достижением технологического суверенитета и структурной адаптацией экономики Российской Федерации, в общем объеме инвестиций Отношение инвестиций организации в проекты, связанные с достижением технологического суверенитета и структурной адаптацией экономики Российской Федерации, к общей сумме управленческих расходов организации			Учет не ведется
69	Общее количество климатически уязвимых объектов в общем количестве объектов основных средств, находящихся на балансе организации Доля климатически уязвимых объектов в общем количестве объектов основных средств, находящихся на балансе организации			Не применимо
70	Доля объектов, для которых проведена количественная и (или) качественная оценка климатических рисков			Не применимо
71	Эффективность мер по адаптации к изменению климата и (или) экономическая эффективность мер по адаптации к изменению климата, реализуемых в рамках корпоративных планов, стратегий или программ, нацеленных на адаптацию к изменению климата (при наличии)			Не применимо
72	Возможный ущерб от воздействия климатических рисков			Не применимо
73	Полученные рейтинги ответственного ведения бизнеса (ЭКГ-рейтинг (ESG-рейтинг), рейтинги устойчивого развития), включение организации в индексы и (или) ренкинги в сфере устойчивого развития и ответственного ведения бизнеса			ЭКГ-рейтинг 105 баллов
Показатели, отражающие участие организации в повышении благосостояния общества и стратегическом развитии Российской Федерации, не включенные в иные разделы				
74	Расходы организации на программы поддержки семьи и родительства Доля расходов организации на программы поддержки семьи и родительства в общей сумме управленческих расходов организации			Более 31 млн рублей в 2025 году было потрачено Компанией на материальную поддержку работников при рождении ребенка. Учет доли в общей сумме управленческих расходов не ведется
75	Доля расходов организации на мероприятия по охране труда и промышленную безопасность в общей сумме управленческих расходов организации			Учет не ведется
76	Расходы организации на поддержку здоровья работников и представителей местного населения, всего: ■ расходы организации на поддержку здоровья работников; ■ расходы организации на поддержку здоровья представителей местного населения; Доля расходов организации на поддержку здоровья работников и представителей местного населения к общей сумме управленческих расходов организации			Учет не ведется

№	Показатель	Раздел отчета	Стр.	Примечания
77	Расходы организации на развитие инфраструктуры здравоохранения Доля расходов организации на развитие инфраструктуры здравоохранения в общей сумме управленческих расходов организации			Учет не ведется
78	Расходы организации на поддержку социально незащищенных групп населения Доля расходов организации на поддержку социально незащищенных групп населения в общей сумме управленческих расходов организации			Более 24 млн рублей было потрачено Компанией в 2025 году на поддержку детей-сирот; детей, оставшихся без попечения родителей; людей с ограниченными возможностями здоровья; НКО, деятельность, которых направлена на помощь социально незащищенных групп населения. Учет доли в общей сумме управленческих расходов не ведется
79	Расходы организации на поддержку массового спорта Доля расходов организации на поддержку массового спорта в общей сумме управленческих расходов организации			Более 14 млн рублей потрачено Компанией в 2025 году на частичную компенсацию сотрудникам расходов на приобретение фитнес-абонемента. Учет доли в общей сумме управленческих расходов не ведется
80	Расходы организации, направленные на поддержку образования, всего: ■ на поддержку общеобразовательных организаций ■ на поддержку организаций, реализующих программы среднего профессионального образования ■ на профессиональную ориентацию детей и молодежи ■ на поддержку дополнительного образования для детей и молодежи ■ на поддержку организаций высшего образования			Учет не ведется
81	Расходы организации на инициативы и проекты, направленные на формирование традиционных российских духовно-нравственных и культурно-исторических ценностей Доля расходов организации на инициативы и проекты, направленные на формирование традиционных духовно-нравственных и культурно-исторических ценностей, в общей сумме управленческих расходов организации			Учет не ведется
82	Расходы организации на добровольческую (волонтерскую) деятельность Доля расходов организации на добровольческую (волонтерскую) деятельность в общей сумме управленческих расходов организации			Более 3,5 млн рублей потратила Компания в 2025 году на поддержку волонтерских инициатив. Учет доли в общей сумме управленческих расходов не ведется
83	Расходы организации на развитие инфраструктуры в сфере культуры, искусства и народного творчества Доля расходов организации на развитие инфраструктуры в сфере культуры, искусства и народного творчества в общей сумме управленческих расходов организации			Неприменимо
84	Расходы организации на улучшение жилищных условий работников (представителей) местных сообществ Доля расходов организации на улучшение жилищных условий работников (представителей) местных сообществ в общей сумме управленческих расходов организации			Неприменимо
85	Расходы организации на повышение благоустройства и комплексное развитие городов и других населенных пунктов Доля расходов организации на повышение благоустройства и комплексное развитие городов и других населенных пунктов в общей сумме управленческих расходов организации			Неприменимо

№	Показатель	Раздел отчета	Стр.	Примечания
86	Расходы организации на повышение качества дорожной сети Доля расходов организации на повышение качества дорожной сети в общей сумме управленческих расходов организации			Неприменимо
87	Отношение расходов организации на реализацию мероприятий, связанных с охраной окружающей среды, в общей сумме управленческих расходов организации			Учет не ведется
88	Расходы на корпоративные программы негосударственного пенсионного обеспечения и (или) долгосрочных сбережений, всего ■ Расходы на корпоративные программы негосударственного пенсионного обеспечения и (или) долгосрочных сбережений, на одного работника Доля расходов на корпоративные программы негосударственного пенсионного обеспечения и (или) долгосрочных сбережений в общей сумме управленческих расходов организации			Корпоративные программы негосударственного пенсионного обеспечения и долгосрочных сбережений отсутствуют
89	Расходы организации на проекты по повышению туристической привлекательности территории Российской Федерации Доля расходов организации на проекты по повышению туристической привлекательности территории Российской Федерации в общей сумме управленческих расходов организации			Неприменимо
90	Отношение инвестиций организации в проекты, связанные с достижением технологического суверенитета и структурной адаптацией экономики Российской Федерации, в общей сумме управленческих расходов организации			Учет не ведется
91	Общие расходы организации на научные исследования и (или) опытно-конструкторские разработки Доля расходов на научные исследования и (или) опытно-конструкторские разработки в общей сумме управленческих расходов организации			Учет не ведется
92	Расходы организации на проекты по разработке и внедрению российских решений в сфере информационных технологий, включая решения, связанные с хранением и обработкой данных, направленных на импортозамещение, в том числе реализуемые стартапами			Учет не ведется
93	Отношение расходов организации на проекты по разработке и внедрению российских решений в сфере информационных технологий, направленных на импортозамещение, в том числе реализуемые стартапами, в общей сумме управленческих расходов организации			Учет не ведется
94	Расходы организации на обеспечение информационной безопасности Отношение расходов организации на обеспечение информационной безопасности в общей сумме управленческих расходов организации			Учет не ведется
95	Отношение расходов организации на обеспечение цифровой безопасности в общей сумме управленческих расходов организации			Учет не ведется

Приложение 9. Глоссарий

APT-атака	От англ. Advanced Persistent Threat (целевая сложная кибератака). Это целенаправленная, сложная в техническом плане и скрытая кибератака, в рамках которой злоумышленники собирают конфиденциальные данные или наносят значительный ущерб компании или определенному человеку
BEC	От англ. Business Email Compromise (компрометация деловой электронной почты) — вид мошеннической атаки, при которой злоумышленник выдает себя за сотрудника, руководителя или контрагента компании в деловой переписке, чтобы добиться перевода денежных средств, передачи данных или иных действий в ущерб компании
DDoS	От англ. Distributed Denial of Service (распределенная атака типа «отказ в обслуживании»). Атака, при которой множество устройств одновременно направляют поток запросов на сервер, сервис или сеть, чтобы перегрузить их и сделать недоступными для пользователей
DLL Hijacking	От англ. Dynamic Link Library Hijacking (подмена динамической библиотеки) — техника атаки, при которой злоумышленник подменяет или размещает вредоносную DLL-библиотеку так, что легитимная программа загружает ее вместо штатной и выполняет вредоносный код
DPI	От англ. Deep Packet Inspection (глубокий анализ трафика). Технология анализа сетевого трафика, позволяющая исследовать не только заголовки пакетов, но и их содержимое для выявления угроз, фильтрации данных и контроля передачи информации
EDR	От англ. Endpoint Detection and Response (обнаружение и реагирование на угрозы на конечных устройствах). Класс решений информационной безопасности, предназначенных для мониторинга конечных устройств, выявления подозрительной активности, расследования инцидентов и реагирования на них
IoT	От англ. Internet of Things (интернет вещей). Сеть взаимосвязанных физических устройств, оснащенных датчиками, программным обеспечением и средствами связи для обмена данными между собой, с облачными системами и другими цифровыми платформами
LLM	От англ. Large Language Model (большая языковая модель). Модель искусственного интеллекта, обученная на больших массивах текстовых данных и способная понимать и генерировать естественный язык, а также выполнять связанные с текстом задачи
Решения MDR	От англ. Managed Detection and Response (управляемое обнаружение и реагирование). Решения для автоматического обнаружения и анализа инцидентов безопасности в инфраструктуре с помощью телеметрии и передовых технологий машинного обучения

OCR	От англ. Optical Character Recognition (оптическое распознавание символов). Технология преобразования текста на изображениях, сканах или фотографиях в машиночитаемый формат для дальнейшей обработки, хранения и поиска
OT-инфраструктура	От англ. Operational Technology (операционные технологии). Совокупность систем, оборудования и программного обеспечения, которые управляют физическими процессами в промышленности, энергетике, транспорте и на других объектах критической инфраструктуры
POSA-карты	От англ. Point of Sale Activation. Продукт, который активируется в точке продаж
SOC	От англ. Security Operations Center (центр мониторинга и реагирования на инциденты информационной безопасности). Выделенная функция или подразделение, которое в непрерывном режиме отслеживает события информационной безопасности, выявляет угрозы и координирует реагирование на инциденты
TIP	От англ. Threat Intelligence Platform (платформа аналитики киберугроз). Платформа для сбора, обогащения, анализа и использования данных о киберугрозах, включая индикаторы компрометации, сведения о злоумышленниках и их тактиках
Vehicle-to-Everything	От англ. Vehicle-to-Everything (обмен данными транспортного средства со всем окружением). Технология обмена информацией в реальном времени между транспортным средством и другими объектами: автомобилями, дорожной инфраструктурой, пешеходами, сетями и облачными системами
XDR	От англ. Extended Detection and Response (расширенное обнаружение и реагирование). Класс систем информационной безопасности, предназначенных для автоматического проактивного выявления угроз на разных уровнях инфраструктуры, реагирования на них и противодействия сложным атакам
АСУ ТП	Автоматизированная система управления технологическим процессом — Комплекс программных и аппаратных средств, предназначенных для автоматизации, мониторинга и управления технологическими процессами на производстве и в промышленной инфраструктуре
Вайперы	От англ. Wiper malware (вредоносные программы для уничтожения данных). Отдельная разновидность программ-шифровальщиков, цель которых — безвозвратное уничтожение данных, восстановление после такой атаки становится невозможным

Вендор	От англ. Vendor (поставщик, производитель). Компания, которая разрабатывает, производит и (или) поставляет продукты, решения или услуги под собственным брендом
Вирусы, черви, троянцы	Распространенные типы вредоносных программ: вирусы внедряются в файлы и распространяются при их запуске, черви распространяются самостоятельно, трояны маскируются под легитимное программное обеспечение
Кибersталкинг	Систематическое преследование человека, группы лиц или компании, их запугивание и (или) домогательство с использованием интернета и других электронных средств коммуникации. Кибersталкингом могут заниматься как родственники и знакомые жертвы, так и организации и посторонние люди
Кликер-игры	От англ. Clicker games / Idle games (кликер-игры). Жанр цифровых игр, основанный на многократных простых действиях пользователя или автоматическом накоплении игровых ресурсов
Конечные точки, конечные устройства	Физические устройства, подключенные к корпоративной или иной сети и способные обмениваться данными с другими системами: компьютеры, ноутбуки, смартфоны, серверы, виртуальные машины и встроенные устройства
Майнинг	Процесс создания новых блоков информации о совершенных с определенной криптовалютой (например, биткойн) транзакциях и добавления их в блокчейн. Каждый новый блок содержит информацию о транзакциях, произошедших с момента создания предыдущего блока. Цель майнинга — подтверждение транзакций с единицами криптовалюты (токенами) и добавление новых единиц в систему (которые являются прибылью майнеров)

Поколение Z	От англ. Generation Z — поколение людей, родившихся ориентировочно с середины 1990-х до начала 2010-х годов и выросших в условиях широкого распространения цифровых технологий и интернета
Реверс-инжиниринг	От англ. Reverse Engineering — обратная разработка кода. Это процесс анализа машинного кода программы, который ставит своей целью понять принцип работы, восстановить алгоритм, обнаружить недокументированные возможности программы и т. п.
Стилер	От англ. Stealer (вредоносная программа для кражи данных). Вредоносная программа, которая незаметно собирает большое количество конфиденциальной информации с зараженных устройств, например логины и пароли, данные платежных карт
Хакатоны	Соревнования или интенсивные командные мероприятия, в ходе которых участники за ограниченное время создают прототипы цифровых решений, продуктов или сервисов
Эксплойт	От англ. Exploit. Вредоносный код, который использует ошибки или недостатки системы безопасности для распространения киберугроз

Приложение 10. Контактная информация

GRI 2-3

По всем вопросам, связанным с отчетом об устойчивом развитии, обращайтесь к **Марии Лосюковой, руководителю проектов устойчивого развития:**

CSR@kaspersky.com

Почтовый адрес центрального офиса:

125212, Россия, Москва,
Ленинградское шоссе, д. 39а, стр. 3,
БЦ «Олимпия Парк»

+7 495 797-87-00,
+7 495 737-34-12

Сайт Компании:
www.kaspersky.com

Для общих вопросов:
info@kaspersky.com

Контакты для прессы:
empr@kaspersky.com

Контактная информация:
https://www.kaspersky.ru/about/contact