

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.

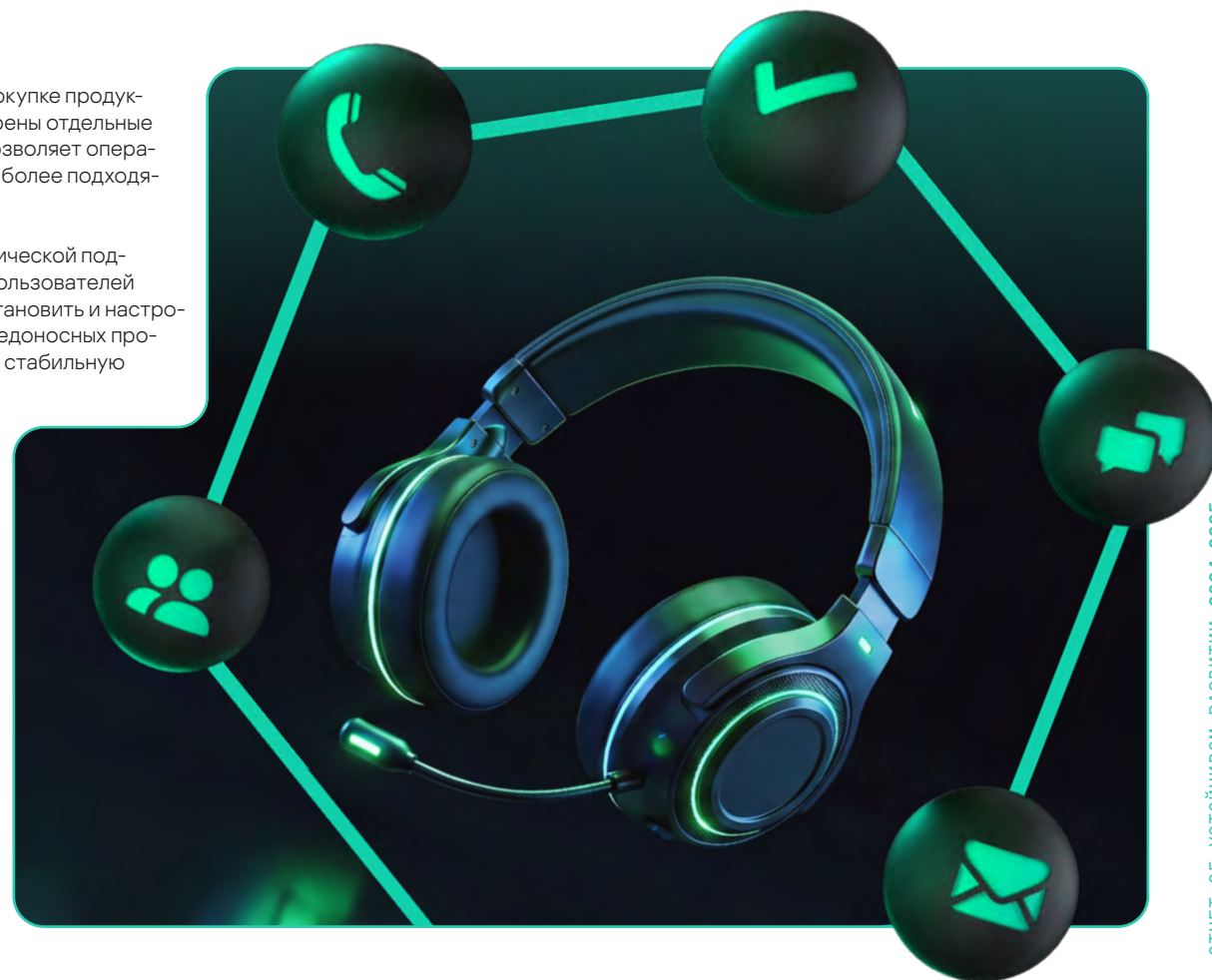
Клиенты Компании имеют доступ к круглосуточной технической поддержке, в том числе в формате удаленной помощи для пользователей потребительских продуктов. Специалисты помогают установить и настроить решения, провести проверку системы на наличие вредоносных программ и устранить технические неполадки, обеспечивая 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 Bounty¹

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 информацию² 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 IT, 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

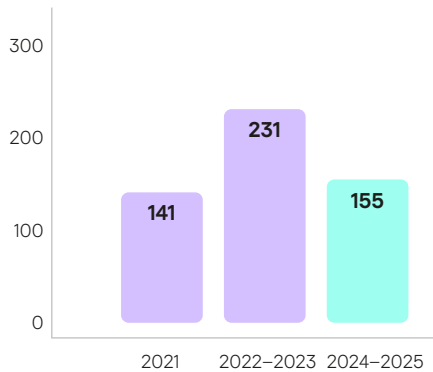
SASB TC-SI-520-a.1

«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 троллями¹.

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.



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.

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

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



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, обеспеченных 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 кода¹.

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 сторонам². 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 этического 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 года¹ 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 взаимодействия 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 этического 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.