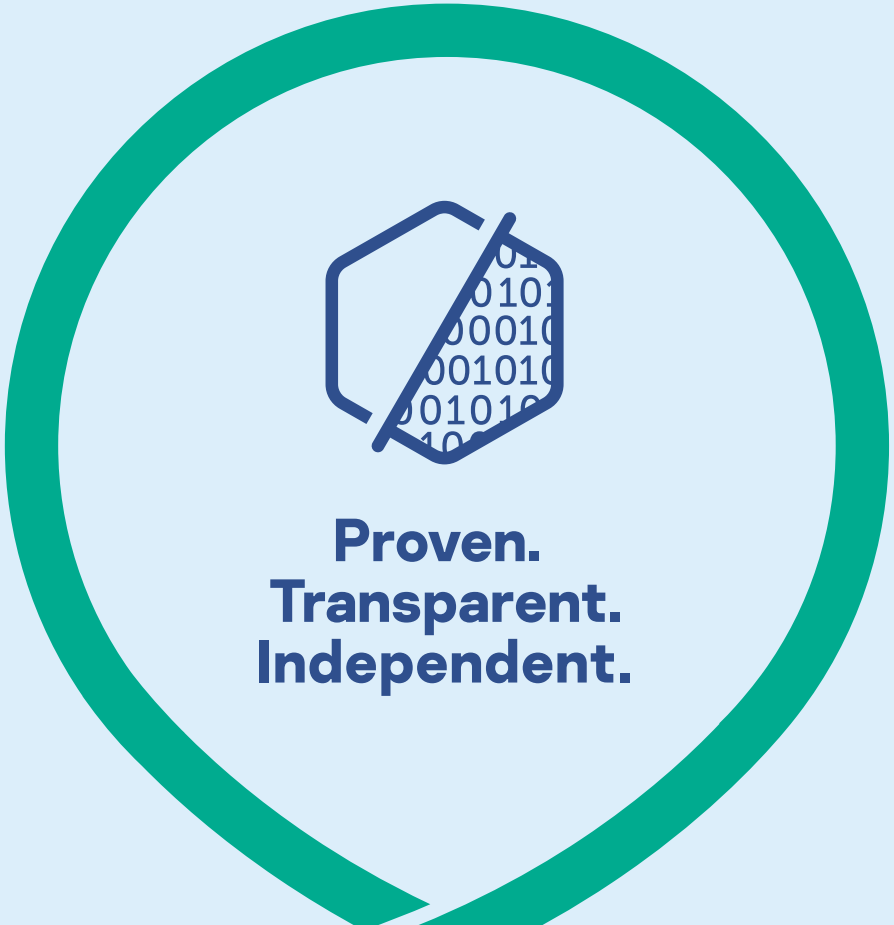
# Global Transparency Initiative

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) — комплекс мер, с помощью которых мы обеспечиваем прозрачность и надежность своих продуктов, а также процессов разработки и бизнес-процессов. Благодаря GTI корпоративные клиенты, партнеры и регуляторы могут посетить наши специализированные центры, чтобы ознакомиться с исходным кодом продуктов Компании, получить разъяснения о наших принципах работы с данными. А сотрудники, получая обратную связь от экспертного сообщества, понимают, что именно нам нужно совершенствовать в вопросах открытости, зрелости процессов и как обеспечивать при этом безопасность продуктов.

# Как возникла и развивалась GTI

Изначально «Лаборатория Касперского» запустила глобальную инициативу по информационной открытости (GTI) в ответ на запросы регулирующих органов, которые интересовались деталями работы наших продуктов: процессом обработки данных, местом их хранения и другими аспектами. С 2017 года мы работаем над пакетом инициатив, направленных на укрепление доверия со стороны наших клиентов и партнеров. Этот пакет включает в себя создание центров прозрачности, проведение независимых аудитов по безопасности и надежности процессов разработки, а также инициативу по переносу части нашей инфраструктуры для обработки вредоносных и подозрительных файлов в дата-центры в Швейцарии.

В дальнейшем в рамках GTI был принят еще ряд мер:

- внедрен независимый анализ исходного кода, программных обновлений и правил обнаружения угроз;
- внедрена независимая оценка процесса безопасной разработки и стратегии по минимизации рисков в цепочке поставщиков и в программном обеспечении;
- открыты центры прозрачности (Transparency Centers) по всему миру;
- усовершенствована программа bug bounty[1] за обнаружение наиболее серьезных уязвимостей в программном обеспечении «Лаборатории Касперского»;
- проведены обучающие семинары по безопасности цепочек поставок и методикам оценки надежности продуктов ИКТ[2];
- создана дополнительная инфраструктура в Швейцарии для хранения и обработки вредоносных и подозрительных файлов, поступающих от пользователей в нашу облачную систему Kaspersky Security Network;
- продолжалась публикация отчетов с информацией о том, сколько запросов на получение данных поступает в Компанию от правоохранительных органов и государственных структур;
- продолжалось развитие образовательных программ, таких как Cyber Capacity Building Program, направленных на повышение квалификации специалистов в области безопасности ИКТ-продуктов.

В 2023 году «Лаборатория Касперского» отметила пятилетие Глобальной инициативы по информационной открытости. Сегодня GTI продолжает эволюционировать, адаптируясь к меняющимся условиям и требованиям рынка кибербезопасности.

## Результаты работы GTI за пять лет

**> $8,4 млн**
инвестиции в развитие GTI с 2018 года

**2 дата-центра**
в Цюрихе

**11**
центров прозрачности по всему миру

**60 ревью**
продуктов Компании в центрах прозрачности

**2**
независимых аудита SOC 2 и на соответствие ISO 27001 ежегодно

**> $81 тысячи**
выплачено за 59 репортов об ошибках в рамках bug bounty

[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] ИКТ — информационные и коммуникационные технологии.

# Как работает GTI

GRI 3-3

Global Transparency Initiative — это не просто набор мероприятий. Это стратегическое направление, целью которого является создание надежного, безопасного и прозрачного цифрового пространства для всех участников.

## Основные элементы GTI

1

### Обзор исходного кода для клиентов и регуляторов

- Одним из ключевых элементов GTI является независимая верификация кода продуктов «Лаборатории Касперского». Кроме того, заинтересованные лица могут получить информацию об исходном коде основных продуктов Компании и наших принципах работы с данными.

2

### Сотрудничество с экспертами

- Другая важная часть GTI — активное сотрудничество с независимыми экспертами и организациями. Мы приглашаем специалистов из разных стран мира для проверки наших систем и продуктов, что добавляет еще больше уверенности в их надежности.

3

### Обучение и просвещение

- Global Transparency Initiative способствует просвещению в области кибербезопасности. «Лаборатория Касперского» активно участвует в различных инициативах, направленных 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 убедить наших корпоративных клиентов, пользователей, партнеров и регуляторов рынка в безопасности и высоком качестве наших продуктов и технологий, мы постоянно совершенствуем GTI, открываем все больше данных о наших процессах, проходим аудиты и сертификации. Благодаря обратной связи от наших стейкхолдеров мы понимаем, какие аспекты требуют особого внимания в вопросах открытости, зрелости процессов и каким образом мы можем обеспечивать при этом безопасность наших продуктов.

TC-SI-220-a.4

## # Решения

### Переносим данные в защищенные дата-центры

Одним из первых шагов Глобальной инициативы по информационной открытости был запуск процесса релокации обработки и хранения файлов. Для этого в 2018 году мы создали два дата-центра в Швейцарии, в которых действуют строгие правила защиты данных. За пять лет в оборудование этих центров, куда Компания перенесла данные своих пользователей, было инвестировано $8,4 млн. Благодаря этому сегодня в Цюрихе успешно действуют два центра обработки вредоносных и подозрительных файлов, поступающих от пользователей на добровольной основе в облачную систему Kaspersky Security Network. Здесь мы обрабатываем и храним данные, связанные с киберугрозами, от пользователей из Европы, Северной и Латинской Америки, Ближнего Востока, а также ряда стран Азиатско-Тихоокеанского региона.

# Открываем новые центры прозрачности

Чтобы дать нашим корпоративным клиентам, партнерам и государственным регуляторам, отвечающим за кибербезопасность, возможность проверить надежность решений Компании, изучив их исходный код, а также узнать больше о наших внутренних процессах, мы создаем центры прозрачности.

Первый такой центр был открыт в Цюрихе в ноябре 2018 года. За пять лет действия GTI Компания создала 11 таких центров — в Бразилии, Италии, Японии, Малайзии, Нидерландах, Руанде, Саудовской Аравии, Сингапуре, Испании, Швейцарии и США. Четыре из них были открыты с июля 2022 года до конца 2023 года.

Мы постоянно расширяем спектр возможностей, предлагаемых в центрах прозрачности. Ранее для ознакомления предлагался только исходный код флагманских продуктов для домашних пользователей и бизнеса. В июле 2023 года стал доступным обзор исходного кода всех решений on-premise для корпоративных клиентов. Вскоре в центрах можно будет увидеть результаты самосертификации продуктов Компании, включая такие элементы, как проектная документация и модели угроз. Это соответствует рекомендациям проекта европейского Закона о киберустойчивости.

**11 центров прозрачности** работают по всему миру

## Итоги 2022–2023 годов

**4 новых центра прозрачности** открыты — в Руанде, Саудовской Аравии, Италии и Нидерландах

Центр прозрачности в Саудовской Аравии стал **первым на Ближнем Востоке**, а центр в Руанде — **первым в Африке**

**34 визита** в центры проведено по всему миру

Расширен перечень продуктов, доступных для аудита в центрах

| США | Бразилия | Испания | Нидерланды | Швейцария | Италия | Саудовская Аравия | Сингапур | Малайзия | Япония | Руанда |
|---|---|---|---|---|---|---|---|---|---|---|
| Вуберн | Сан-Паулу | Мадрид | Утрехт | Цюрих | Рим | Эр-Рияд | Сингапур | Куала-Лумпур | Токио | Кигали |

## Проходим независимую оценку

В 2023 году мы успешно прошли

**аудит SOC 2**

второго типа

В рамках Глобальной инициативы по информационной открытости «Лаборатория Касперского» регулярно получает независимую оценку своих внутренних процессов. Так, с 2019 года системы управления данными Компании проходят ежегодную сертификацию в соответствии со стандартом ISO/IEC 27001:2013. Аудит подтверждает безопасность решений Компании. Также с 2019 года «Лаборатория Касперского» регулярно проходит аудит Service Organization Control for Service Organizations (SOC 2).

В 2023 году Компания успешно прошла аудит SOC 2 Type 2. Аудит 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.

## Собираем данные об уязвимостях через программу bug bounty

**59 репортов**

о незначительных уязвимостях получено за пять лет

**$81 750**

выплачено за репорты

С марта 2018 года «Лаборатория Касперского» получила 59 сообщений о незначительных уязвимостях в рамках программы bug bounty, устранила их и на сегодняшний день выплатила независимым исследователям в качестве вознаграждения в общей сложности $81 750.

Максимальный размер вознаграждения в программе bug bounty установлен на уровне до $100 тысяч за обнаружение наиболее серьезных уязвимостей в ПО «Лаборатории Касперского». 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.

## Учим, как оценивать уровень кибербезопасности

**2 организации**

(государственное учреждение и частная компания) прошли тренинги Cyber Capacity Building Program в отчетном периоде

Наша образовательная программа Cyber Capacity Building предназначена для сотрудников частных и государственных компаний, а также университетов, которые хотят получить практические 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]. Этим предложением интересуются представители государственного и частного сектора. За отчетный период две организации прошли тренинги: представители регулирующего органа связи Намибии и частной организации.

## 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 каждые шесть месяцев 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.

Теперь «Лаборатория Касперского» один раз в 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.

# Планы по развитию GTI на 2024 год

К середине 2024 года Компания планирует расширить сеть центров прозрачности, открыв еще как минимум один центр, организовать не менее пяти визитов в центры прозрачности, а также продолжить прохождение международных независимых сертификаций и выпуск отчетов по взаимодействию с правоохранительными органами.

**Наш вклад в разработку этических принципов цифрового развития**

## Представили принципы этичного использования искусственного интеллекта (ИИ) в кибербезопасности

Искусственный интеллект дает большие преимущества для индустрии кибербезопасности, но также несет риски в области приватности и свободы пользователей. В октябре 2023 года на Форуме по управлению интернетом, прошедшем под эгидой Организации Объединенных Наций (ООН), «Лаборатория Касперского» представила свои этические принципы разработки и использования систем на основе машинного обучения, созданные в рамках GTI:

**Прозрачность**

Компания информирует клиентов об использовании технологий машинного обучения в своих продуктах и услугах.

**Безопасность**

Следует использовать широкий спектр мер безопасности для обеспечения качества систем машинного обучения.

**Человеческий контроль**

Он нужен для проверки работы AI/ML-систем при анализе сложных угроз.

**Право на цифровую приватность**

Компания применяет ряд технических и организационных мер для защиты данных и систем, чтобы обеспечить цифровую приватность пользователей.

**Приверженность целям кибербезопасности**

Инструменты машинного обучения должны использоваться исключительно в целях кибербезопасности.

**Открытость к диалогу**

Мы готовы обмениваться передовым опытом в области этичного использования алгоритмов машинного обучения со всеми заинтересованными сторонами.

### Что в результате?

Мы рассказали нашим партнерам, пользователям, профессиональному сообществу, как мы обеспечиваем надежность работы систем машинного обучения, и призвали других участников отрасли присоединиться к диалогу и выработать общие этические принципы.