

Защита данных



Мы уважаем право наших клиентов на конфиденциальность и защищаем их данные. Наша цель — исключить их утечки у пользователей «Лаборатории Касперского».

~4 **тысячи**
сотрудников прошли курс по работе с данными клиентов

>3 **тысяч**
запросов на обработку данных пользователей в 2023 году

GRI 418-1

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.

GRI 3-3

Наш подход к защите данных

Мы делаем все, чтобы обеспечить защиту данных наших клиентов по всему миру. Такая информация — ценный актив для современных компаний. Мы защищаем персональную информацию¹ наших клиентов от возможных несанкционированных изменений, компрометации или потери. Для этого мы используем лучшие в своем классе технологии и принимаем следующие меры безопасности.

- Жизненный цикл безопасной разработки ПО обеспечивает создание защищенных продуктов и оперативное исправление уязвимостей.

- Надежное шифрование гарантирует безопасный обмен данными между устройством пользователя и облаком.
- Цифровые сертификаты позволяют выполнять легитимную и безопасную аутентификацию серверов и обновление приложений.
- Данные хранятся раздельно на множестве серверов с ограниченными правами и строгими политиками доступа.
- Данные анонимизируются различными методами, среди которых удаление данных учетных записей из переданных URL-адресов, получение хеш-сумм вредоносных файлов вместо самих файлов, сокрытие IP-адресов пользователей и т. д.

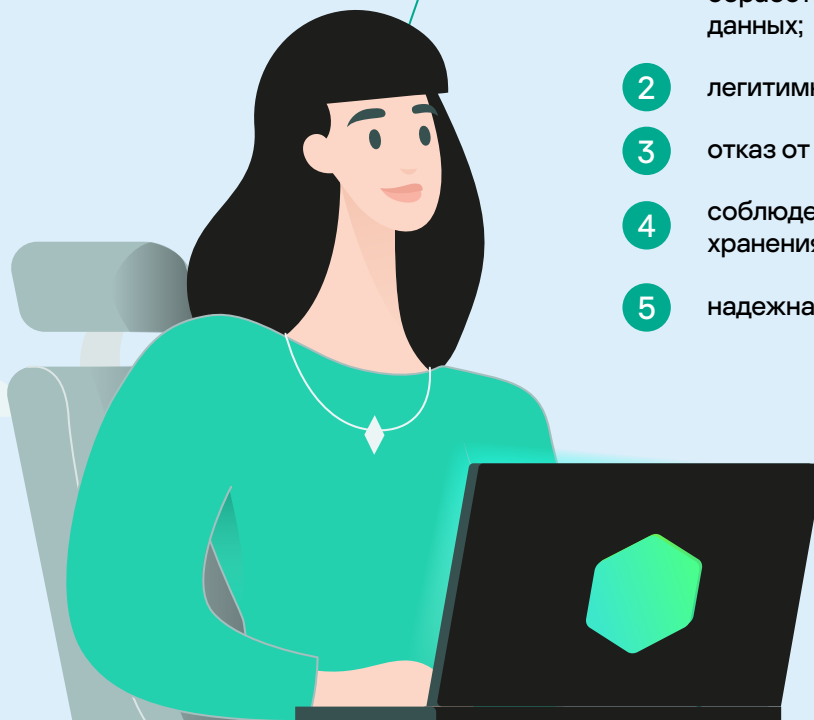
¹ Персональная информация — любая информация, относящаяся к физическому лицу, включая Ф.И.О., номера телефонов, адрес, IP-адрес, адрес электронной почты и т. д.

Как мы защищаем данные по всему миру и предотвращаем их утечки

TC-SI-220-a.1

TC-SI-230-a.2

Мы руководствуемся ключевыми принципами работы с данными согласно европейскому регламенту по защите данных (EU General Data Protection Regulation [GDPR](#)), 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 PIPL¹, CCPA², LGPD³, PDPD⁴, 152-ФЗ⁵ и др.



Пять ключевых принципов работы с данными клиентов:

- 1 законность и прозрачность обработки данных для субъектов данных;
- 2 легитимность целей обработки;
- 3 отказ от сбора избыточных данных;
- 4 соблюдение предельных сроков хранения данных;
- 5 надежная защита данных.

Мы стремимся свести число инцидентов к нулю. За отчетный период у нас не было нарушений законодательства о персональных данных или утечек данных. Это стало возможным благодаря постоянному обучению сотрудников, внедренным технологиям защиты информации и стандартизации работы с данными. В отчетном периоде мы обновили наши требования к обработке данных, а также провели адаптацию этих требований под законодательство разных стран.

Самую актуальную информацию, включая количество удовлетворенных запросов от наших пользователей, мы собираем в [отчете прозрачности](#). Документ находится в открытом доступе, обновляется и публикуется каждые шесть месяцев.

¹ Закон КНР о защите персональных данных (Personal Information Protection Law of the People's Republic of China).

² Закон штата Калифорния о защите персональных данных потребителей (California Consumer Privacy Act).

³ Общий закон о защите данных Бразилии (Lei Geral de Proteção de Dados).

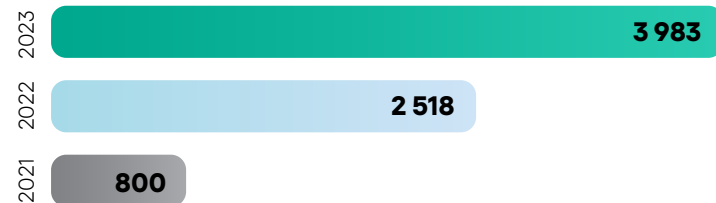
⁴ Закон Вьетнама о защите персональных данных (Personal Data Protection Decree).

⁵ Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Обучаем правилам работы с данными

В «Лаборатории Касперского» действует курс повышения осведомленности для сотрудников, непосредственно вовлеченных в процессы обработки данных клиентов. В 2023 году этот курс прошли 3 983 человека — все европейские работники Компании и сотрудники по всему миру, вовлеченные в процессы обработки и защиты данных клиентов. Это на 58% больше, чем годом ранее.

Количество сотрудников, прошедших курс по работе с данными клиентов



Оценка рисков

Мы используем риск-ориентированный подход, направленный на защиту данных наших пользователей. Оценка рисков выполняется на всех этапах: при внедрении новых систем, разработке новых решений, расследовании инцидентов. В каждом случае мы заранее анализируем, какие риски могут возникнуть при обработке данных клиентов, и сводим эти риски к минимуму.

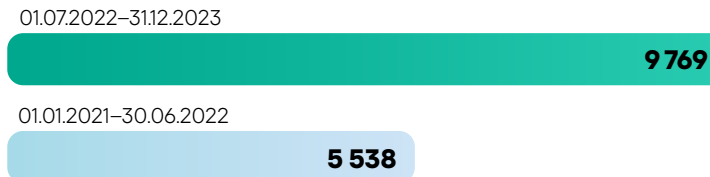
Требования GDPR и региональные законодательства учитывают риски, которым могут подвергнуться пользователи. Нивелировать репутационные и финансовые риски для Компании нам помогает стандарт ISO/IEC 27001.

Оперативно реагируем на запросы пользователей

ТС-SI-220-a.1

Количество ежемесячных запросов на обработку данных, которые «Лаборатория Касперского» получает от пользователей, иногда доходит до тысячи. 90% этих запросов — требования об удалении их данных из баз Компании.

Количество обработанных Компанией запросов пользователей на обработку их данных¹, штук



Пользователи также просят предоставить выгрузку своих данных и сведения о том, какая информация о них хранится и где. В отчетном периоде (с 1 июля 2022 года по конец 2023 года) мы успешно обработали 9 769 обращений, а в период с 1 января 2021 года по 30 июня 2022 года — 5 538. Мы наблюдаем тенденцию к увеличению количества таких запросов как в Европе, так и по всему миру. Это происходит по двум причинам: повышение осведомленности пользователей о своих правах и принятие новых законов о персональных данных.

Наша цель — предоставлять всю необходимую информацию о данных пользователям, чтобы они могли доверять нашей Компании и продуктам. В рамках налаженного процесса получения и обработки запросов мы создаем [отчеты прозрачности](#), в которых фиксируем количество и типы запросов, поступающих к нам от клиентов. Мы обновляем и публикуем такие отчеты каждые шесть месяцев.

Как и большинство компаний, мы работаем с данными пользователей и в таргетированной рекламе². Согласно GDPR, данные, полученные через cookies³, считаются персональными, а значит, при их сборе нужно соблюдать соответствующие правила. Единые строгие политики по получению согласий для сбора информации на сайтах применены в Бразилии, Великобритании и во всей Европе. В остальных странах мы собираем минимальные данные для предоставления релевантной информации для наших потенциальных клиентов.

Для взаимодействия с потребителями, клиентами и поставщиками в «Лаборатории Касперского» работает форма обратной связи на официальном сайте:

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

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

¹ Согласно отчетам прозрачности.

² Таргетированная реклама — один из ключевых инструментов маркетинга, когда для продвижения товаров и услуг используют персональные данные пользователей, собранные с помощью различных веб-сайтов, приложений и соцсетей.

³ Cookies — небольшие файлы, хранящиеся на компьютерах и гаджетах, с помощью которых сайт запоминает информацию о посещениях пользователя.

Предотвращаем утечки данных

GRI-418-1

TC-SI-220-a.1

TC-SI-230-a.1

TC-SI-220-a.2

TC-SI-220-a.3

За соблюдение принципов и процедур в области безопасности данных в Компании отвечает Privacy Team.

Команда, в которую вошли сотрудники подразделений IT, R&D, ИБ и интеллектуальной собственности, сформировалась в 2016 году, когда внедрялись требования GDPR. Privacy Team приводила в соответствие европейскому регламенту все процессы в Компании. Сейчас команда обеспечивает выполнение функций обработки данных в таких направлениях, как консультирование, организационные вопросы и контроль.

Начиная с 2019 года «Лаборатория Касперского» ежегодно проходит сертификацию своих систем по работе с данными на соответствие требованиям международного стандарта [ISO/IEC 27001](#), подтверждая их высокий уровень защиты. В отчетном периоде область аудита информационных систем была значительно расширена. Мы наняли новых сотрудников и сформировали новое подразделение, с помощью которого в 2023 году было проведено 388 внутренних аудитов.

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 действительна для сервисов обработки данных, расположенных в дата-центрах в Цюрихе, Франкфурте-на-Майне, Глаттбурге, Торонто, Москве и Пекине.

Запуск новой системы учета

В отчетном периоде мы завершили масштабный проект — запустили новую систему учета процессов и сервисов обработки данных, созданную силами команды разработчиков «Лаборатории Касперского». В ней учитывается, какие сервисы обрабатывают данные клиентов, в каких бизнес-процессах они используются, кто контроллер (оператор) и процессор (обработчик) данных, какие данные в системе хранятся, как долго, на каком основании, в каком объеме, в каких странах и т. д. Новая система готова к работе, и в нее уже перенесено 80% данных.

0

серьезных нарушений законодательства о персональных данных и значительных утечек

0

убытков в результате судебных разбирательств из-за нарушения конфиденциальности за отчетный период

388

внутренних аудитов

на сертификацию соответствия ISO/IEC 27001 в 2023 году

Наши планы на 2024 год

- Выставление обновленных требований по обработке и защите данных ко всем сервисам, в которых обрабатываются данные клиентов.
- Проведение консультаций команд по обновленным требованиям.
- Проведение аудитов эффективности сервисов в области обработки и защиты данных пользователей.