О «Лаборатории Касперского»

kaspersky

Апрель 2021

У нас простая и понятная миссия – мы строим безопасный мир

Используя свой опыт и достижения, мы хотим сделать цифровое пространство защищённым – чтобы каждый мог наслаждаться теми безграничными возможностями, которые ему способны предложить технологии.

Евгений Касперский,
генеральный директор

Кратко о «Лаборатории Касперского»

Факты о компании

Главное

Основана в **1997** году, возглавляется Евгением Касперским

Работает почти в **200** странах и территориях мира

Разрабатывает **инновационные** IT-решения для защиты корпоративных и домашних пользователей

Цифры

> 14 миллионов активаций продуктов в год

> 4 000 высококвалифицированных специалистов

685 миллионов долларов – глобальная неаудированная выручка в 2019 году

Достижения и признание в отрасли

Один из пяти крупнейших в мире производителей решений для конечных устройств*

Обладает наградой **Gartner Peer Insights Customers' Choice 2020** в категории Endpoint Detection & Response Solutions**

Обладает наградой «Продукт года» от AV-Comparatives***

>400 000 000 пользователей по всему миру защищены нашими технологиями

* Компания заняла 5-е место в рейтинге IDC 'Worldwide Endpoint Security Market Shares, 2018: Large Vendors Write a New Market Narrative (Doc #US45055519 May 2019).
** Рейтинг Gartner Peer Insights отражает субъективные мнения конечных пользователей, основанные на их личном опыте. Количество опубликованных отзывов и общий рейтинг конкретного вендора не могут считаться позицией Gartner или кого-либо из её партнёров. https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions.
*** Продукт Kaspersky Internet Security в шестой раз получил награду «Продукт года». (Product of the Year 2020).

География

200 стран и территорий

34 региональных офиса

Северная Америка

Мексика
США

Южная Америка

Бразилия

Африка

ЮАР

Австралия

Европа

Австрия
Великобритания
Германия
Дания
Израиль
Испания
Италия
Нидерланды
Польша
Португалия
Россия (HQ)
Румыния
Франция
Чехия
Швейцария

Азия

Гонконг
Индия
Казахстан
Китай
Малайзия
ОАЭ
Сингапур
Турция
Южная Корея
Япония

Центры прозрачности

Цюрих, Швейцария
Мадрид, Испания
Сан-Паулу, Бразилия
Куала-Лумпур, Малайзия
Нью-Брансуик, Канада
(готовится к открытию)

Наша роль в мировом сообществе по IT-безопасности

Мы участвуем в расследованиях и операциях по противодействию киберугрозам совместно с мировым сообществом по информационной безопасности, международными организациями, такими как Интерпол и Европол, правоохранительными органами и центрами CERT по всему миру.

Мы сотрудничаем с Интерполом: предоставляем своих экспертов, проводим тренинги, делимся аналитическими данными о последних киберинцидентах.

Совместно с девятью другими организациями мы создали коалицию по борьбе со сталкерским ПО – коммерческими программами для слежки, которые используются в том числе инициаторами домашнего насилия.

Член консультативной группы Европола по безопасности в интернете Европейского центра по борьбе с киберпреступностью (EC3).

Совместно с Cigref мы выступаем сопредседателями шестой рабочей группы в рамках инициативы «Парижский призыв к доверию и безопасности в киберпространстве».

Член Консорциума промышленного Интернета (Industrial Internet Consortium), который помогает организациям максимально быстро и удобно интегрировать физические и цифровые среды.

Проект No More Ransom

NO MORE RANSOM!

С 2016 года «Лаборатория Касперского» помогает пользователям защищаться от программ-шифровальщиков с помощью инициативы No More Ransom, реализуемой совместно с полицией Нидерландов, Европолом и McAfee. Проект представляет собой веб-портал www.nomoreransom.org, где можно получить бесплатные инструменты для восстановления данных, а также больше узнать о программах-шифровальщиках и исходящих от них угрозах.

- **Более 100 бесплатных инструментов для дешифровки файлов**
- **160+ партнёров по всему миру**
- **Сайт доступен на 37 языках**

Наши принципы прозрачности ведения бизнеса

Данные, отправляемые в «Лабораторию Касперского», критически важны для защиты пользователей, они надёжно защищены и не атрибутируются конкретным людям

Мы находим и нейтрализуем угрозы независимо от их происхождения или предназначения

Мы сотрудничаем с правительствами и правоохранительными органами разных стран в целях борьбы с киберугрозами

Мы придерживаемся принципов честной и прозрачной разработки технологий и решений

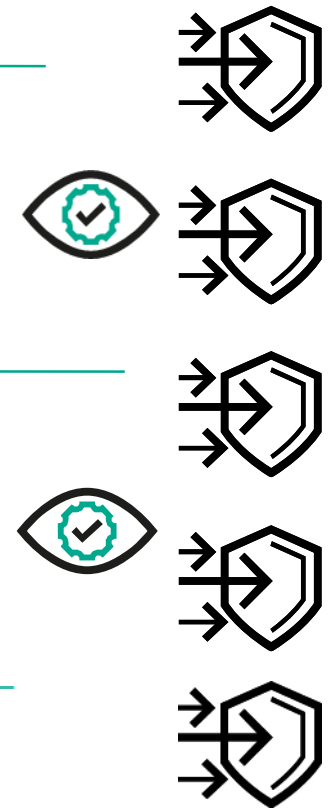
Мы сотрудничаем с другими представителями индустрии IT-безопасности в рамках совместных расследований киберинцидентов

Наша глобальная инициатива по информационной открытости

В 2017 году «Лаборатория Касперского» запустила Глобальную инициативу по информационной открытости (Global Transparency Initiative), основная цель которой — привлечь широкое сообщество по кибербезопасности к верификации продуктов, внутренних процессов и бизнес-операций компании.

Инициатива предусматривает ряд конкретных мер и шагов:

- **Независимый анализ кода и обновлений**
- **Внешний аудит процесса разработки и сертификации**
- **Программа Bug Bounty**
- **Перенос R&D инфраструктуры**
- **Обучающая программа Cyber Capacity Building Program**



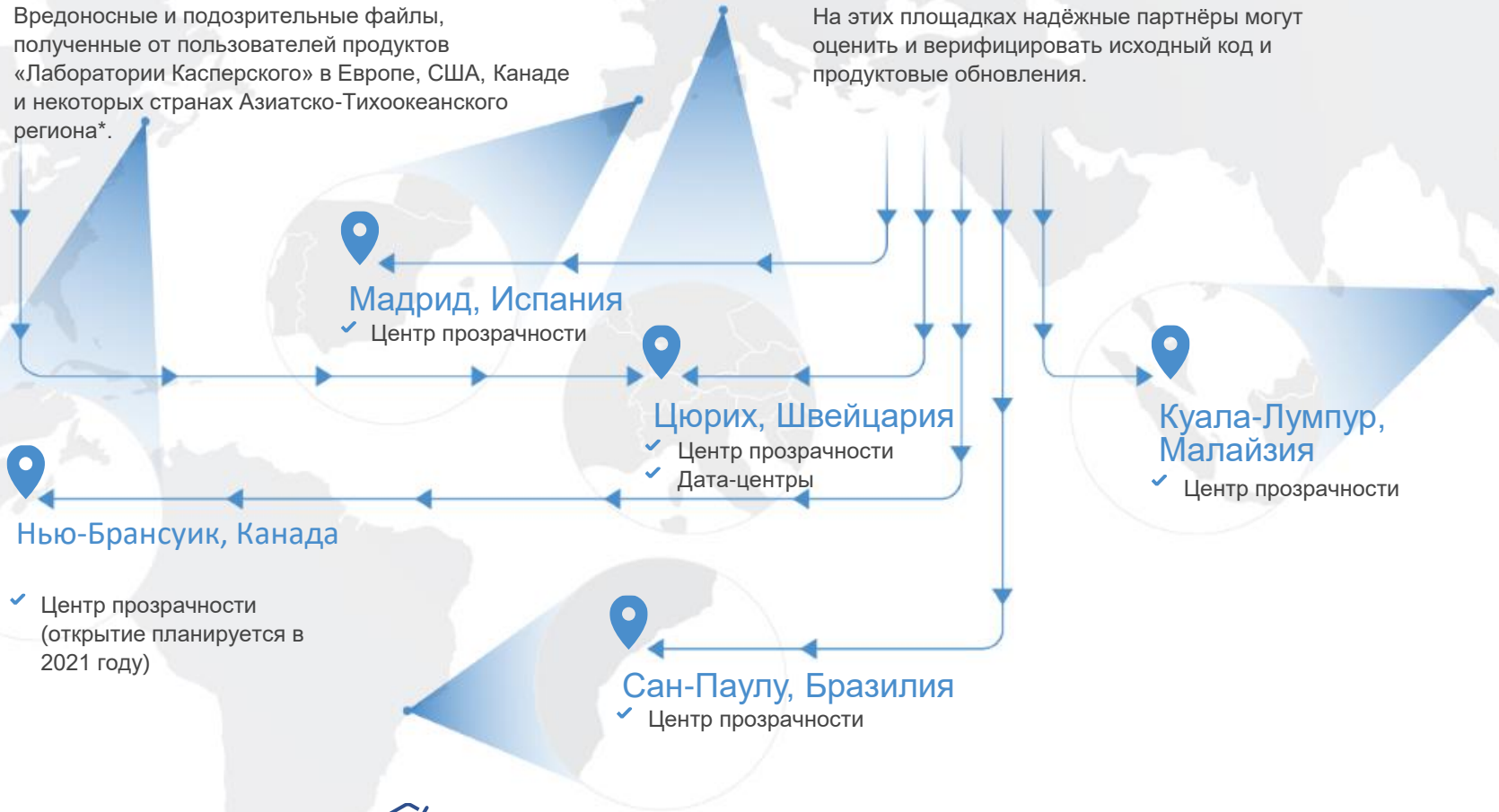
Глобальная инициатива по информационной открытости

Хранение и обработка пользовательских данных

Вредоносные и подозрительные файлы, полученные от пользователей продуктов «Лаборатории Касперского» в Европе, США, Канаде и некоторых странах Азиатско-Тихоокеанского региона*.

Центры прозрачности

На этих площадках надёжные партнёры могут оценить и верифицировать исходный код и продуктовые обновления.



Мадрид, Испания
- Центр прозрачности

Цюрих, Швейцария
- Центр прозрачности
- Дата-центры

Куала-Лумпур, Малайзия
- Центр прозрачности

Нью-Брансуик, Канада
- Центр прозрачности (открытие планируется в 2021 году)

Сан-Паулу, Бразилия
- Центр прозрачности

Независимый обзор

Сторонняя оценка внутренних процессов с целью проверки решений «Лаборатории Касперского» на целостность.
В 2019 году компания успешно прошла аудит по контрольным процедурам в сервисных организациях – Service Organization Control for Service Organizations (SOC 2) Type 1.

Программа Bug Bounty

Инициатива предусматривает привлечение сторонних исследователей и выплату им вознаграждения в случае обнаружения критических брешей в продуктах «Лаборатории Касперского».

Также мы поддерживаем проект Disclose.io, который представляет собой безопасную площадку (Safe Harbor) для исследователей уязвимостей, обеспокоенных негативными юридическими последствиями своих раскрытий.

kaspersky BRING ON THE FUTURE

Proven. Transparent. Independent.

*Австралия, Новая Зеландия, Япония, Бангладеш, Бруней, Камбоджа, Индия, Индонезия, Южная Корея, Лаос, Малайзия, Непал, Пакистан, Филиппины, Сингапур, Шри-Ланка, Таиланд и Вьетнам.

«Лаборатория Касперского»: Digital Trust

- Хранение и обработка данных европейских пользователей в дата-центре в Швейцарии
- Частная облачная инфраструктура (KPSN), созданная с учётом высочайших стандартов приватности

- Аудит SOC2 от одной из компаний «Большой четвёрки» подтверждает, что в «Лаборатории Касперского» применяются сильные механизмы контроля разработки антивирусных баз
- Продукты «Лаборатории Касперского» демонстрируют высокие результаты по итогам 62 независимых тестов

- Центры прозрачности в Цюрихе, Мадриде, Сан-Паулу и Куала-Лумпуре, где можно ознакомиться с исходным кодом. В 2021 году планируется открытие центра в Нью-Брансуике (Канада)
- Ответственное закрытие уязвимостей в рамках программы Bug Bounty
- Независимое подтверждение соответствия нормам GDPR
- Частная и независимая компания с 23-летней историей
- Приоритет компании – в непрерывном развитии новых технологий
- Сильная команда экспертов по кибербезопасности + R&D специалисты, которые составляют треть всего штата

SOC 2 аудит

«Лаборатория Касперского» успешно прошла аудит SOC 2 Type 1 в соответствии со стандартом SSAE 18. Аудит проводила одна из компаний «Большой четвёрки».

Этот аудит подтверждает, что процесс разработки и выпуска правил распознавания угроз (антивирусных баз) защищён от неавторизованного вмешательства благодаря сильным механизмам контроля безопасности.

SOC

The Service Organization Controls (SOC) — всемирно признанный стандарт отчёта для системы управления рисками кибербезопасности, разработанный Американским институтом дипломированных общественных бухгалтеров (American Institute of Certified Public Accountants, AICPA).

Сертификация ISO 27001

«Лаборатория Касперского» получила сертификат ISO/IEC 27001:2013. Аудит был проведён компанией TÜV AUSTRIA.

Сертификат подтверждает, что системы компании, включая Kaspersky Security Network, соответствуют требованиям международного стандарта систем менеджмента информационной безопасности ISO/IEC 27001. Сертификат распространяется на инфраструктуру компании, расположенную в дата-центрах в Цюрихе, Франкфурте-на-Майне, Торонто и Москве.

ISO/IEC 27001
Наиболее широко распространённый стандарт в области информационной безопасности, подготовленный и опубликованный Международной организацией по стандартизации (ISO).

Программа Bug Bounty

«Лаборатория Касперского» реализует свою программу bug bounty с 2016 года и делает это в партнёрстве с известной платформой HackerOne. Компания также поддерживает проект Disclose.io, который представляет собой безопасную площадку (Safe Harbor) для исследователей уязвимостей, обеспокоенных негативными юридическими последствиями своих раскрытий.

Кто может участвовать

- Независимые исследователи, достигшие как минимум 13-летнего возраста.
- Любые исследователи за исключением сотрудников «Лаборатории Касперского» и связанных с ней организаций, а также членов их семей.

Продукты, доступные для анализа

- Kaspersky Internet Security 2019
- Kaspersky Endpoint Security 11
- Kaspersky Endpoint Security for Linux
- Kaspersky Password Manager
- Kaspersky Secure Connection

Вознаграждение

- **$100 000**
  за обнаружение и ответственное раскрытие наиболее серьёзных уязвимостей (качественный отчёт с проверкой концепции).
- **$5 000 – $20 000**
  за обнаружение уязвимостей, позволяющих реализовать менее серьёзные варианты удалённого выполнения кода.
- **$1 000 – $5 000**
  за обнаружение брешей в ПО, позволяющих повысить локальные права доступа или приводящих к раскрытию конфиденциальных данных.

Ландшафт угроз

Эксперты

>4 000 высококвалифицированных специалистов

1/3 наших сотрудников – R&D специалисты

40+ ведущих экспертов в сфере IT-безопасности

Наша уникальная команда экспертов по информационной безопасности защищает мир от самых сложных и опасных киберугроз. Накопленная ими база знаний обогащает наши решения и сервисы, выводя их качество на несравненный уровень.

Исследование угроз

Более миллиарда киберугроз

обнаружила «Лаборатория Касперского»
с момента своего основания

10 миллиардов кибератак

обнаружила «Лаборатория Касперского»
в 2020 году

360 тысяч новых вредоносных файлов

обнаруживает «Лаборатория Касперского»
каждый день

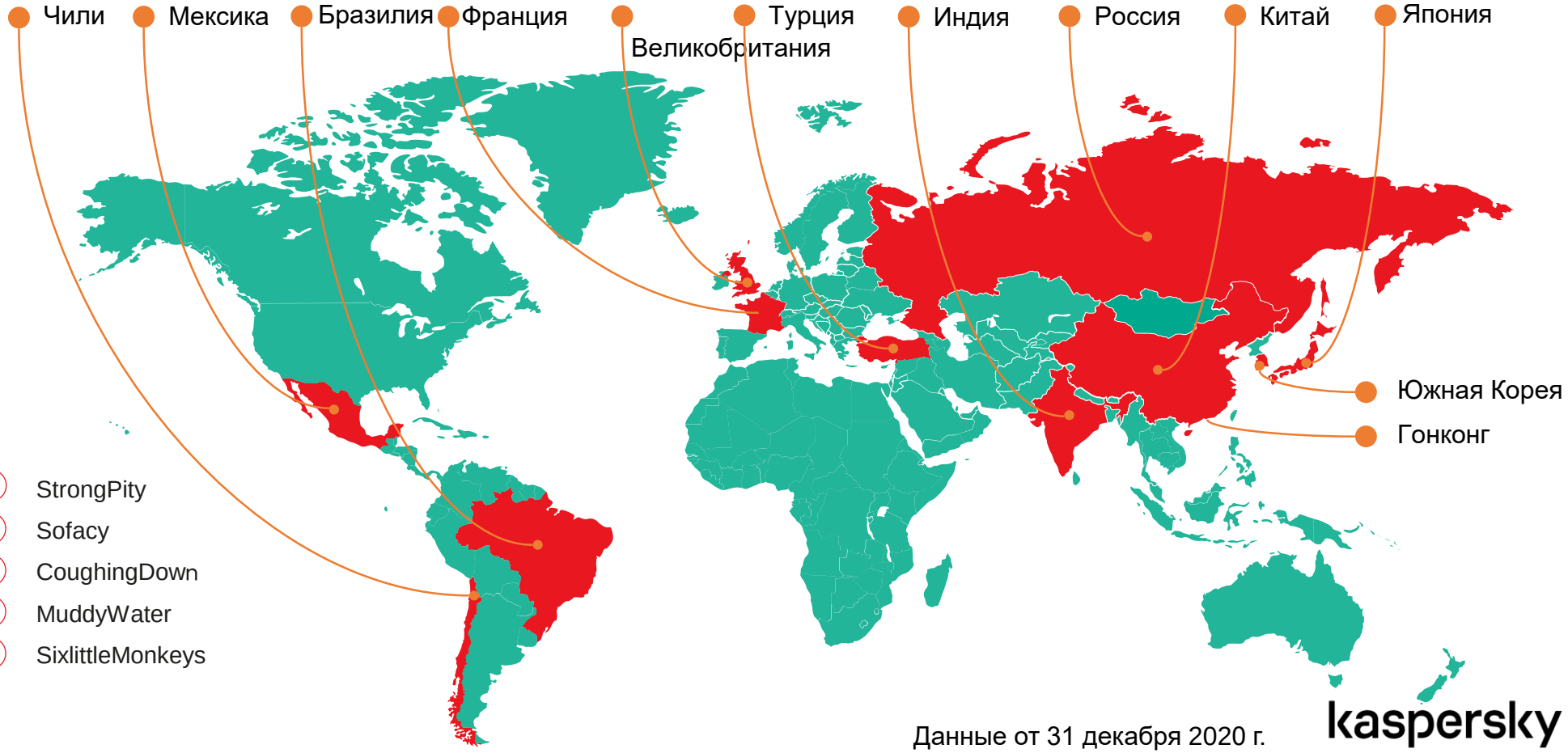
Сложные APT-угрозы в 2020 году

В «Лаборатории Касперского» создан Глобальный центр исследований и анализа угроз, который известен во всём мире благодаря своим раскрытиям и расследованиям наиболее сложных кибератак. Согласно данным этого центра, в 2020 году главной мишенью сложных и хорошо спланированных кибероперацийстали правительственные органы, а наиболее активной группировкой оказалась Lazarus.

Топ-10 целей:

- Правительства
- Банки
- Финансовые институты
- Дипломаты
- Телекоммуникации
- Образование
- Оборонные предприятия
- Энергетика
- Военные ведомства
- IT-компании

Топ 12 атакованных стран:



Топ-10 кибергрупп:

1. Lazarus
2. DeathStalker
3. CactusPete
4. IAmtheKing
5. Transparent Tribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixlittleMonkeys

apt.securelist.com

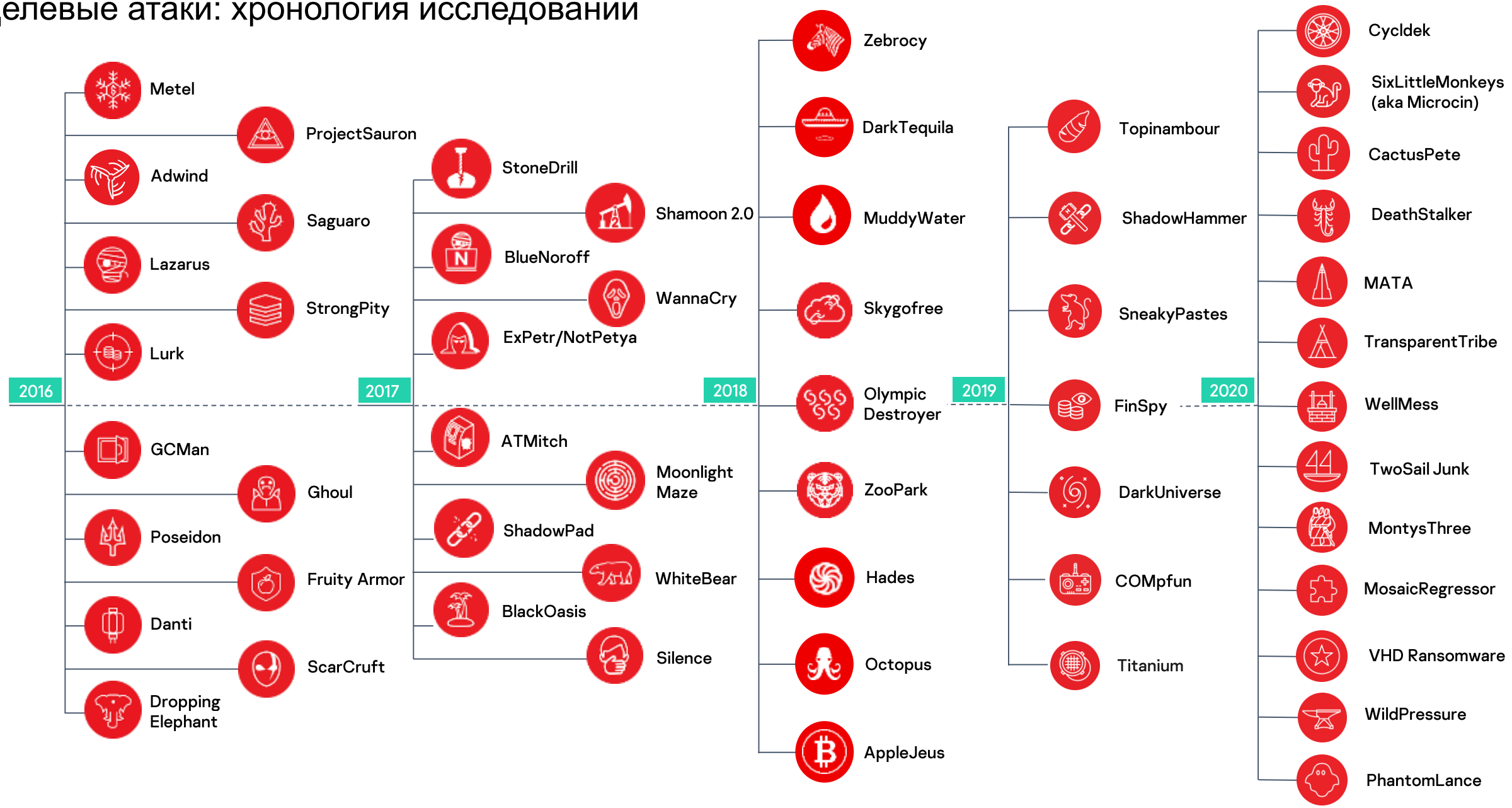
Данные от 31 декабря 2020 г.

kaspersky

Наши главные открытия

	SOFACY	DUQU 2.0	LURK	LAZARUS	PROJECT SAURON	EXPETR/ NOTPETYA	SHADOWPAD	OLYMPIC DESTROYER	SHADOW HAMMER	TAJMAHAL	MOSAICREGRESSOR
Обнаружение	2014	2015	2016	2016	2016	2017	2017	2018	2018	2019	2020
Начало активности	2008	2014	2011	2009	2011	2017	2017	2017	2018	2013	2017
Классификация	ПО для кибершпионажа	Комплексная платформа для кибератак	Киберпреступная операция	Кибершпионаж и саботаж, финансовые атаки	ПО для кибершпионажа	Кампания по уничтожению данных	Модульная платформа для кибератак	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа
Описание	Группа также известна как Fancy Bear, Sednit, STRONTIUM и APT28. Отличается высоким профессионализмом Подозревается в связях с группой Miniduke. Активно использует уязвимости нулевого дня.	Крайне сложная вредоносная платформа, эксплуатирующая до трёх уязвимостей нулевого дня.	Группировка создала сеть заражённых компьютеров, с помощью которых с 2011 года украла более $45 млн из банков и других финансовых организаций. Злоумышленники получали доступ к удалённым банковским сервисам, для того чтобы красть деньги со счетов клиентов.	Предположительно, группировка стояла за атаками на Sony Pictures Entertainment в 2014 году и на Центральный банк Бангладеш в 2016. Ответственна за уничтожение данных и кампании кибершпионажа в отношении многих компаний по всему миру.	Атаки на государственные органы. В каждом случае использовался уникальный набор инструментов, что делает традиционные техники обнаружения почти бесполезными.	Программа-стиратель, притворяющаяся вымогателем. Использовались модифицированные эксплойты EternalBlue и EternalRomance. Некоторые признаки указывают на связь ExPetr и BlackEnergy.	Одна из самых известных атак на цепочки поставок. Было атаковано серверное ПО NetSarang, используемое в сотнях крупных компаний по всему миру. Атакующие развернули в сетях жертв платформу, которая позволяла получить гибкие возможности удаленного доступа.	Продвинутая кибергруппировка, атаковавшая организаторов, поставщиков и партнёров Зимних Олимпийских игр в Пхеньяне с помощью разрушительного сетевого червя. Отличительной особенностью этой группы является использование множества ложных флагов.	В результате сложной атаки на цепочку поставщиков разработчика популярной утилиты для обновления ПО вредоносная программа была загружена почти на 1 млн компьютеров Windows под видом обновления ПО. При этом зловред был подписан легитимным сертификатом.	Технически сложный APT-фреймворк, предназначенный для кибершпионажа. Содержит около 80 вредоносных модулей. Может красть файлы, стоящие в очереди на печать, а также файлы с USB-носителей.	Многоступенчатый модульный фреймворк для кибершпионажа и сбора данных. Он использует буткит для микропрограммы UEFI. Это позволяет атакующим искажать зашифрованные данные без ведома жертвы.
Цели	Военные и государственные организации по всему миру	Заражениям подверглись площадки, на которых проходили высокопоставленные встречи мировых лидеров группы P5+1	Банки, другие финансовые организации и коммерческие компании	СМИ, финансовые организации, казино, разработчики ПО для инвестиционных компаний, криптовалютные бизнесы	В основном государственные организации. Более 30 жертв в России, Иране и Руанде	Распространялась по всему миру, в первую очередь были атакованы компании на Украине, в России и Западной Европе. >50% атакованных — промышленные предприятия	Банковские и финансовые организации, разработчики ПО, СМИ, энергетика и коммунальное хозяйство, страхование, промышленность и строительств, производство и другие отрасли	Организации, имеющие отношение к Зимним Олимпийским играм 2018; европейские организации, изучающие биологические и химические угрозы; финансовые организации в России	Специальные инструкции во вредоносном коде устанавливали в качестве цели 600 систем, определённых по специальным, MAC-адресам	Дипломатические организации	Дипломатические представительства, чья деятельность связана с Северной Кореей

Целевые атаки: хронология исследований



Решения и сервисы «Лаборатории Касперского»

Наши клиенты

Наши решения и сервисы нового поколения доступны самому широкому кругу — от домашних пользователей до крупных предприятий, критически важных инфраструктурных объектов и правительственных организаций.

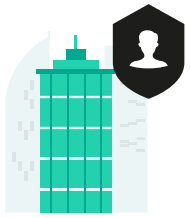
Крупные предприятия

Промышленные объекты

Малый и средний бизнес

Микробизнес

Домашние пользователи



>240 000

корпоративных клиентов по всему миру

>400 000 000

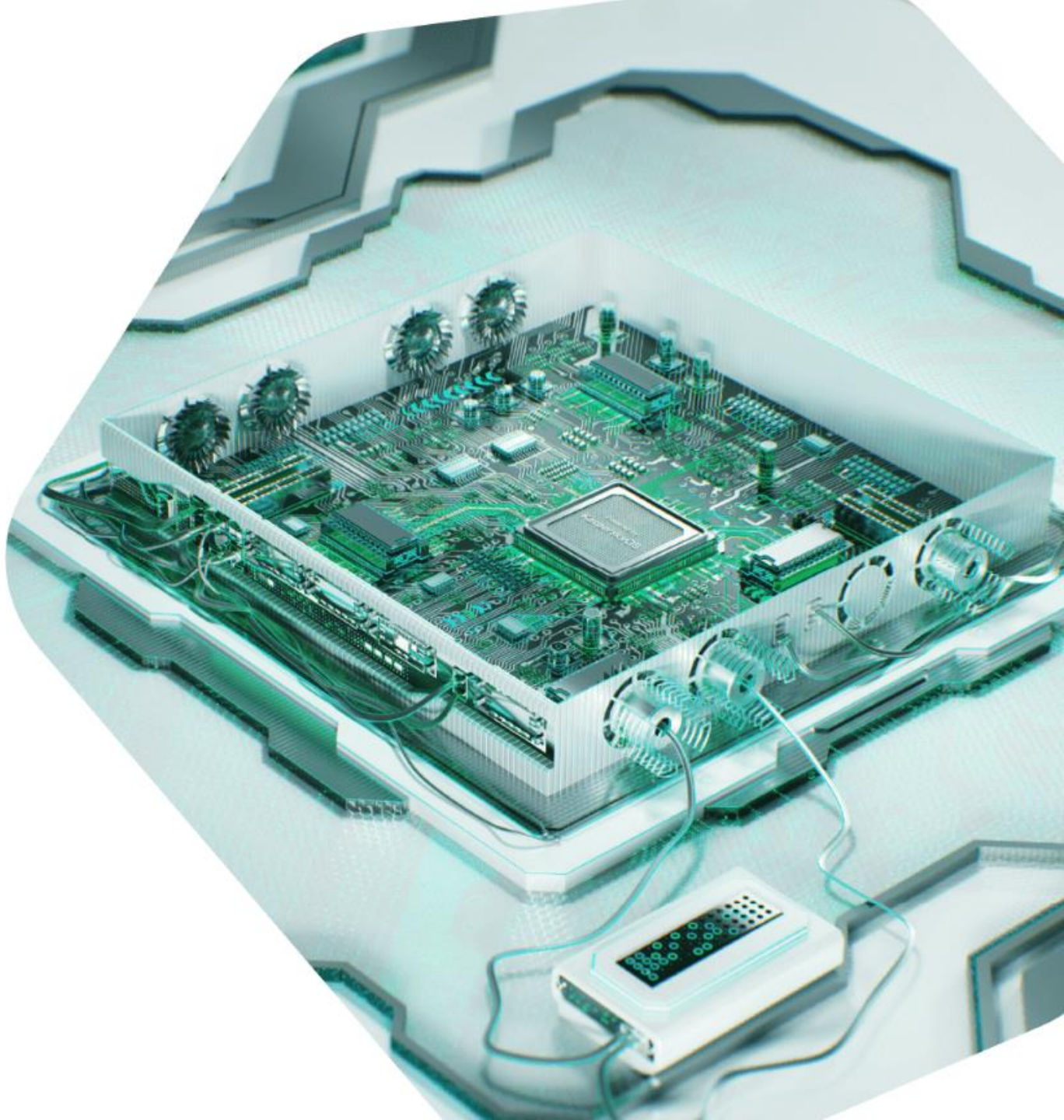
пользователей наших технологий во всем мире

KasperskyOS

создает среду, в которой уязвимости и ошибки кода больше не представляют угрозы

обеспечивает защиту программных и информационных систем от вредоносного кода, вирусов и хакерских атак

Защитный компонент **Kaspersky Security System (KSS)** контролирует взаимодействие между всеми частями системы, делая эксплуатацию уязвимостей бесполезной для злоумышленников



KasperskyOS

- Проприетарное микроядро – разработанное «с нуля» специалистами «Лаборатории Касперского».
- Изначально безопасная система – создана как безопасная, она остаётся безопасной в течение всего своего жизненного цикла
- Статическая настройка безопасности: любое действие, не предусмотренное политиками безопасности, запрещено по умолчанию.
- Бизнес-логика отделена от функций безопасности – это облегчает разработку и поддержку, сокращает время выхода на рынок, повышает безопасность.
- Многоуровневая совместимость – POSIX-совместима (поддержка около 98% POSIX API).
- Поддерживаемая архитектура: Intel x86, x64 и ARM (v6, v7, v8).

KasperskyOS

KasperskyOS — это операционная система для подключённых к интернету встраиваемых систем с особыми требованиями к кибербезопасности.

Телекоммуникации

Транспорт

Интернет вещей

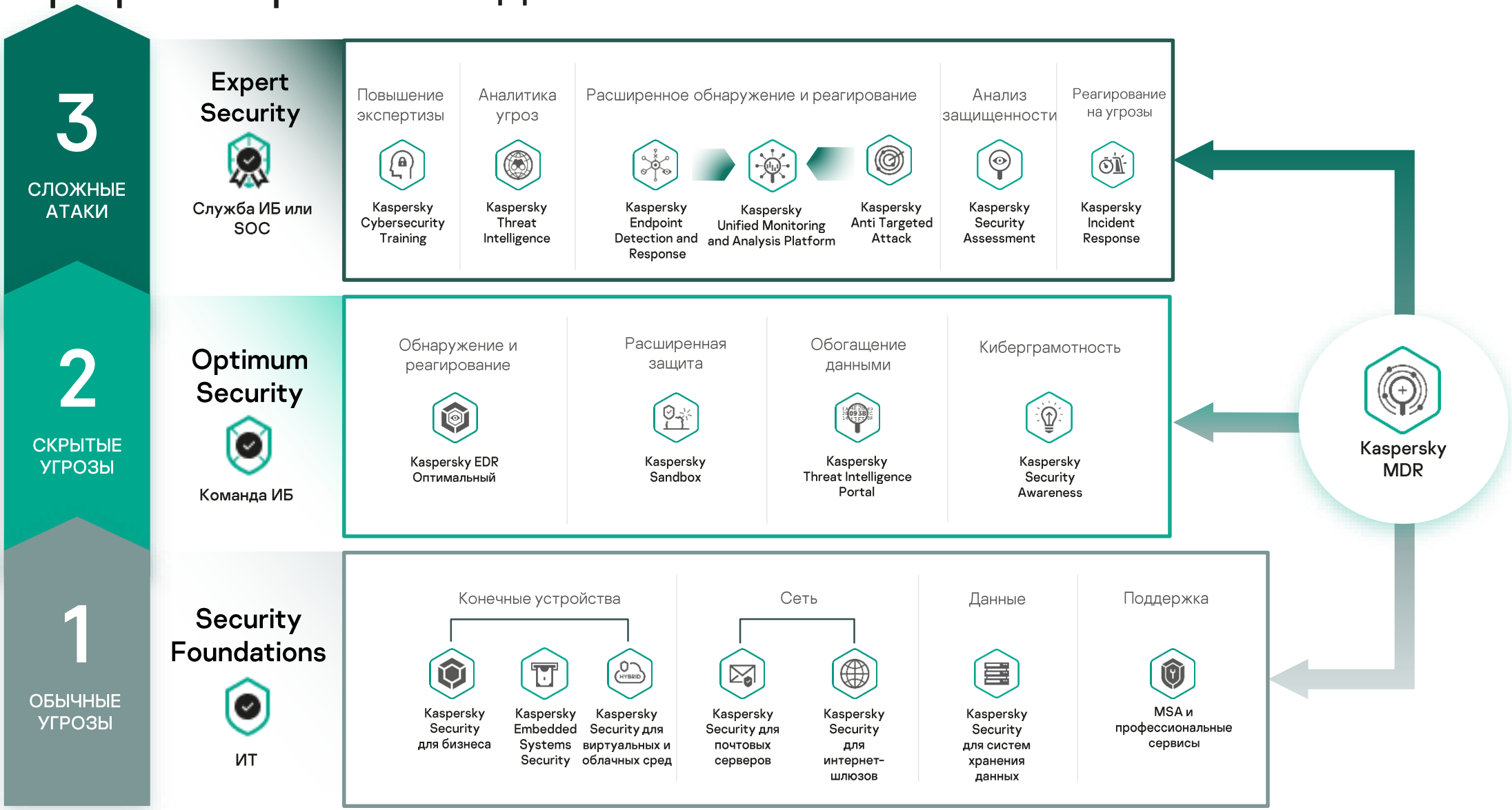
Промышленность

Большие и малые экраны

Kaspersky IoT Secure Gateway

- Обнаружение и классификация устройств
- Безопасная загрузка и обновления
- Доступ через веб-интерфейс
- Сетевой экран
- IPS/IDS
- Система удаленного управления и мониторинга (KSC)
- MQTT-брокер

Портфолио решений для бизнеса



Решения нового поколения для защиты крупного бизнеса

Технологии

Threat Management and Defense

Стратегическое решение для борьбы со сложными угрозами

Контроль и защита рабочих мест

Комплексное, масштабируемое решение нового поколения для защиты рабочих мест

Облачная безопасность

Надёжная защита гибридного облака

Защита SOC-центров

Широкий спектр сервисов – от потоков данных и тренингов до реагирования на киберинциденты, поиска угроз и анализа защищённости

Интернет вещей и встроенная безопасность

Минимизация рисков и борьба с киберугрозами, направленными на интернет вещей и встроенные устройства

Борьба с мошенничеством

Проактивное обнаружение кросс-канального фрода в режиме реального времени

Отрасли

Защита государственных органов

Сервисы и услуги в области кибербезопасности, учитывающие потребности государственных предприятий и ведомств

Защита финансовых учреждений

Инструменты для повышения уровня безопасности финансовых учреждений

Защита транспортных предприятий

Безопасность всех областей транспортной IT-инфраструктуры

Защита телекоммуникационных компаний

Эффективная защита телекоммуникационной инфраструктуры и информационных систем

Защита промышленных предприятий

Специализированная защита для систем промышленного контроля

Защита предприятий здравоохранения

Защита IT-инфраструктуры медицинских учреждений и конфиденциальных данных пациентов

Защита торговых компаний

Защита и проверка на соответствие законодательным нормам POS-терминалов, рабочих станций, мобильных устройств и систем бэк-офиса

Защита блокчейна

Защита криптоэкономики

Промышленная кибербезопасность

KasperskyOS (Безопасная операционная система)

- ✓ Изначально безопасная система
- ✓ Проприетарное микроядро и независимый безопасный движок
- ✓ Кибериммунитет

Authorized to Use CERT℠
CERT is a mark owned by Carnegie Mellon University

Kaspersky ICS CERT

Специалисты Industrial Systems Emergency Response Team предлагают экспертные сервисы и консультационные услуги

Kaspersky Industrial CyberSecurity

Поддерживаемые промышленные конечные узлы:

- ✓ SCADA-серверы
- ✓ SCADA-клиенты
- ✓ Человеко-машинные интерфейсы (HMI)
- ✓ Инженерные рабочие станции
- ✓ Серверы архивных данных
- ✓ OPC-шлюзы

Некоторые поддерживаемые устройства и протоколы

SIEMENS, Schneider Electric, OMRON, Rockwell Automation, MITSUBISHI ELECTRIC, EMERSON, ABB, GE, CODESYS, YOKOGAWA

PRODUCTS

Industrial Endpoint Protection

KICS for Nodes

Возможности защиты конечных узлов:

- ✓ Белые списки приложений
- ✓ Движок для защиты от вредоносного ПО
- ✓ Контроль устройств
- ✓ Мониторинг целостности файлов
- ✓ Защита от эксплойтов
- ✓ Беспроводной контроль доступа
- ✓ Анализ логов
- ✓ Проверка целостности ПЛК
- ✓ Защита от шифровальщиков
- ✓ Сетевой экран

Industrial Anomaly and Breach Detection

KICS for Networks

Возможности контроля целостности сети:

- ✓ Визуализация сети
- ✓ Мониторинг сетевой активности
- ✓ Учёт активов
- ✓ Передовая технология DPI
- ✓ Машинное обучение для обнаружения аномалий
- ✓ Обнаружение удалённого доступа
- ✓ Обнаружение распространения вредоносного ПО
- ✓ Корреляция событий
- ✓ Безопасная запись подозрительных событий
- ✓ Интеграция SOC/SIEM

Centralized security management

Kaspersky Security Center

SERVICES

Training and awareness

Kaspersky® Security Awareness

Kaspersky® Security Trainings

Программы обучения и повышения осведомлённости:

- ✓ Кибербезопасность современных промышленных систем (1 день)
- ✓ Практика промышленной кибербезопасности (1-2 дня)
- ✓ Цифровая криминалистика (4 дня +)
- ✓ Тестирование на проникновение (5 дней)
- ✓ Безопасность интернета вещей (4 дня)
- ✓ CTF-соревнования
- ✓ Подготовка тренеров
- ✓ Интерактивная игра Kaspersky Interactive Protection Simulation (KIPS)

Expert services and intelligence

Kaspersky® Security Assessment

Kaspersky® Incident Response

Kaspersky® Threat Intelligence

Kaspersky® Managed Protection

Экспертные сервисы:

- ✓ Тестирование на проникновение и моделирование угроз
- ✓ Рекомендации по выстраиванию безопасной сетевой архитектуры и управлению ей
- ✓ Реагирование на инциденты и цифровая криминалистика (по запросу или по подписке)
- ✓ Потоки данных о текущем ландшафте промышленных угроз (TTPs, цели, атрибуция)
- ✓ База данных уязвимостей и консультационные услуги

Решения нового поколения для малого и среднего бизнеса

Столь же лёгкий в управлении, как и домашний антивирус

Kaspersky Small Office Security

- Облачная консоль управления
- Защита от финансового мошенничества
- Шифрование и резервное копирование данных
- Создание, хранение и синхронизация паролей

Быстрая защита в условиях ограниченных ресурсов

Kaspersky Endpoint Security Cloud

- Простое управление, отсутствие затрат на покупку дополнительного оборудования
- Защита ПК, файловых серверов, ноутбуков и мобильных устройств
- Предустановленные политики безопасности
- Новейшее, наиболее современное ПО

Защита уровня корпораций

Kaspersky Endpoint Security для бизнеса

- Решение для защиты конечных устройств и автоматизированная песочница
- Защищает сотрудников и компанию от кибератак
- Максимизирует число обработанных инцидентов без дополнительной нагрузки на сотрудников
- Легко масштабируется, подходит для защиты разных сред и платформ

Решения нового поколения для бизнеса

Специализированные решения:

Kaspersky Security для виртуальных и облачных сред

Kaspersky Security для почтовых серверов

Kaspersky Security для Microsoft Office 365

Многоуровневая защита для физических, виртуальных, мобильных сред и серверов

Высочайший уровень обнаружения угроз

Интегрированная платформа безопасности

Управление из единой консоли

Технологии будущего на страже безопасности частных пользователей

Персонализированная защита в сочетании с машинным обучением и другими технологиями нового поколения

Широкий спектр приложений «Лаборатории Касперского» под одним лёгким в управлении аккаунтом

Защищает **приватность** и **данные** пользователей и оптимизирует **производительность** их устройств

Защищает не только устройства:

- обнаружение утечки данных – оповещает пользователя, если учётные данные от его аккаунтов попали в сеть, и даёт советы по защите;
- мониторинг домашней сети Wi-Fi – предупреждает пользователя о подключении новых устройств и сообщит, если к сети подключится посторонний

Быстро работает **на всех платформах** благодаря облачным технологиям

Kaspersky Security Cloud

Доступен на:

Доступно два варианта: Personal и Family

Kaspersky Security Cloud Family включает все, что есть в Personal: антивирус, защиту платежей, менеджер паролей, безопасное соединение. А еще в этой версии решения есть приложение для родительского контроля и к нему можно удаленно подключить до 19 членов семьи, при этом у каждого будет собственная учетная запись.

Безопасность частных пользователей

Мы вдохновляем наших пользователей получать все преимущества от новых технологий — потому что они знают, что мы позаботились об их безопасности.

Защита детей, приватности и мобильных гаджетов

Kaspersky VPN Secure Connection
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Internet Security for Android

Лидеры продаж

Kaspersky Total Security
Win | Android | Mac | iOS

Kaspersky Internet Security
Win | Android | Mac

Бесплатные приложения

Kaspersky QR Scanner
Android | iOS

Kaspersky Battery Life
Android

Kaspersky Security Cloud Free
Win | Android | iOS

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION

*kaspersky.com/top3

62
теста/обзора

45
первых мест

81%
попаданий в топ-3

—

Кибербезопасность сегодня жизненно необходима как отдельному человеку, так и целым организациям. И в связи с этим вопрос доверия к провайдерам становится ключевым. Мы защищаем домашних пользователей и корпоративных клиентов по всему миру, и признание на рынке крайне важно для нас. В 2020 году решения «Лаборатории Касперского» участвовали в 62 независимых тестах и обзорах. В 45 из них наши продукты заняли первые места, и в итоге в 50 случаях оказались в тройке лидеров.

*62 независимых теста, проведённых в 2020 году, в которых продукты «Лаборатории Касперского» сравнивались с продуктами 13 компаний-конкурентов. В тестах приняли участие более 100 вендоров, но только те из них, которые участвовали как минимум в 35% испытаний, представлены в рейтинге топ-3.

Центр инноваций «Лаборатории Касперского»

Центр инноваций «Лаборатории Касперского» – это ключевой элемент нашей стратегии развития, созданный для поощрения корпоративных инноваций и развития сотрудничества компании с блестящими умами в области разработки технологий.

МИССИЯ: Мы постоянно ищем самые передовые проекты, работающие в сфере кибербезопасности, чтобы способствовать созданию и развитию новых бизнес-возможностей, а также расширять наши предложения в разных отраслях. Мы действуем в рамках нашей главной цели – перейти к концепции кибериммунитета мира.

Улучшение существующих продуктов
Проверка новых идей
Новые тенденции

Анализ и минимизация рисков

Увеличение доходов

Выстраивание экосистемы

Создание команды мечты

«Лаборатория Касперского» на рынке

Признание клиентов

«Лаборатория Касперского» вошла в рейтинг Gartner Peer Insights Customers' Choice 2020 в категории "Endpoint Detection and Response".

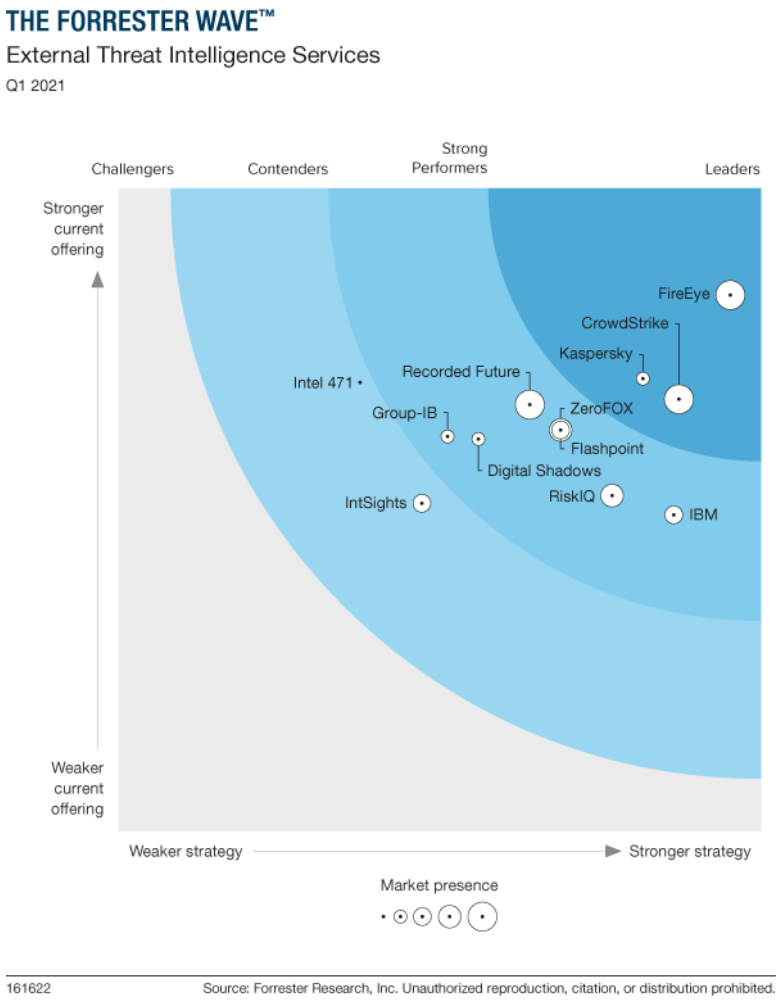
Логотип Gartner Peer Insights Customer Choice является торговой маркой компании Gartner, Inc. и использован с ее разрешения. Рейтинг Gartner Peer Insights отражает субъективные мнения конечных пользователей, основанные на их личном опыте. Количество опубликованных отзывов и общий рейтинг конкретного вендора не могут считаться позицией Gartner или кого-либо из ее партнеров. https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions

Признание клиентов

Платформа «Лаборатории Касперского» для повышения цифровой грамотности получила награду «Выбор клиентов» в регионах EMEA и APAC.

Логотип Gartner Peer Insights Customer Choice является торговой маркой компании Gartner, Inc. и использован с ее разрешения. Рейтинг Gartner Peer Insights отражает субъективные мнения конечных пользователей, основанные на их личном опыте. Количество опубликованных отзывов и общий рейтинг конкретного вендора не могут считаться позицией Gartner или кого-либо из ее партнеров. https://www.kaspersky.ru/enterprise-security/security-awareness.

Сервисы оперативного информирования об угрозах



«Лаборатория Касперского» признана лидером в области сервисов оперативного информирования о киберугрозах по результатам аналитического отчета The Forrester Wave™: External Threat Intelligence Services Q1, 2021.

Сервисы «Лаборатории Касперского» вошли в топ-2.

Признание аналитиков

«Лаборатория Касперского» была признана Frost and Sullivan глобальной компанией года (“Global Company of the Year”) на рынке промышленной кибербезопасности*.

*Результаты отчета Frost and Sullivan 2020 Global Industrial (OT/ICS) Cybersecurity market analysis. Полностью он доступен по ссылке https://www.kaspersky.com/acq-lp/kicsaward2020-ungated.

Признание аналитиков

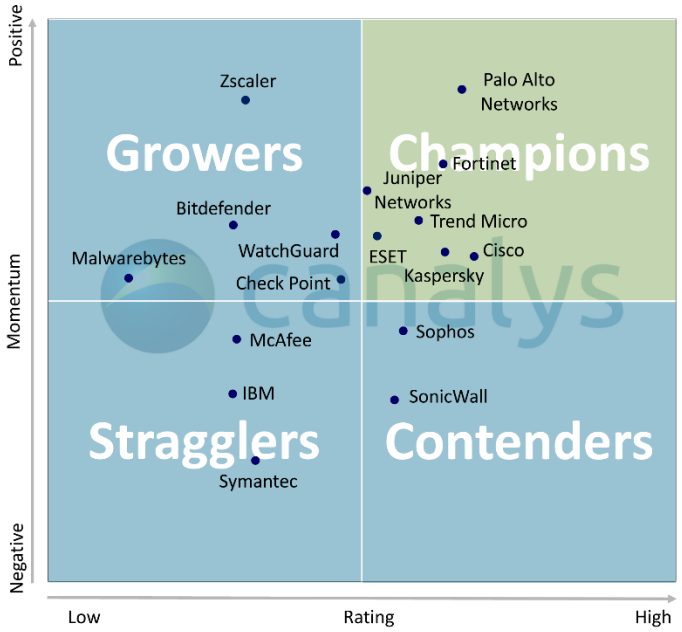
«Лаборатория Касперского» признана ведущим вендором в сфере кибербезопасности по уровню удовлетворенности партнеров среди 11 вендоров по результатам теста Canalys Worldwide Vendor Benchmark*. Компания получила самый высокий рейтинг — 87,8%.

Тест The Canalys Worldwide Vendor Benchmark — это объективное сравнение партнерских программ вендоров в различных сферах, в том числе в кибербезопасности, измеряющее их эффективность по ряду ключевых показателей. «Лаборатория Касперского» получила 679 отзывов о своей программе от партнерского канала, что на 588% больше по сравнению с предыдущим годом.

*Отчет Canalys, декабрь 2020 г.

Признание аналитиков

Global Cybersecurity Leadership Matrix
May 2020



«Лаборатория Касперского» была названа чемпионом (**Champion)** в матрице Canalys Global Cybersecurity Leadership Matrix 2020*.

Чемпионы — это вендоры с наиболее высокими оценками, которые продемонстрировали прогресс в развитии партнерского канала за последние 12 месяцев.

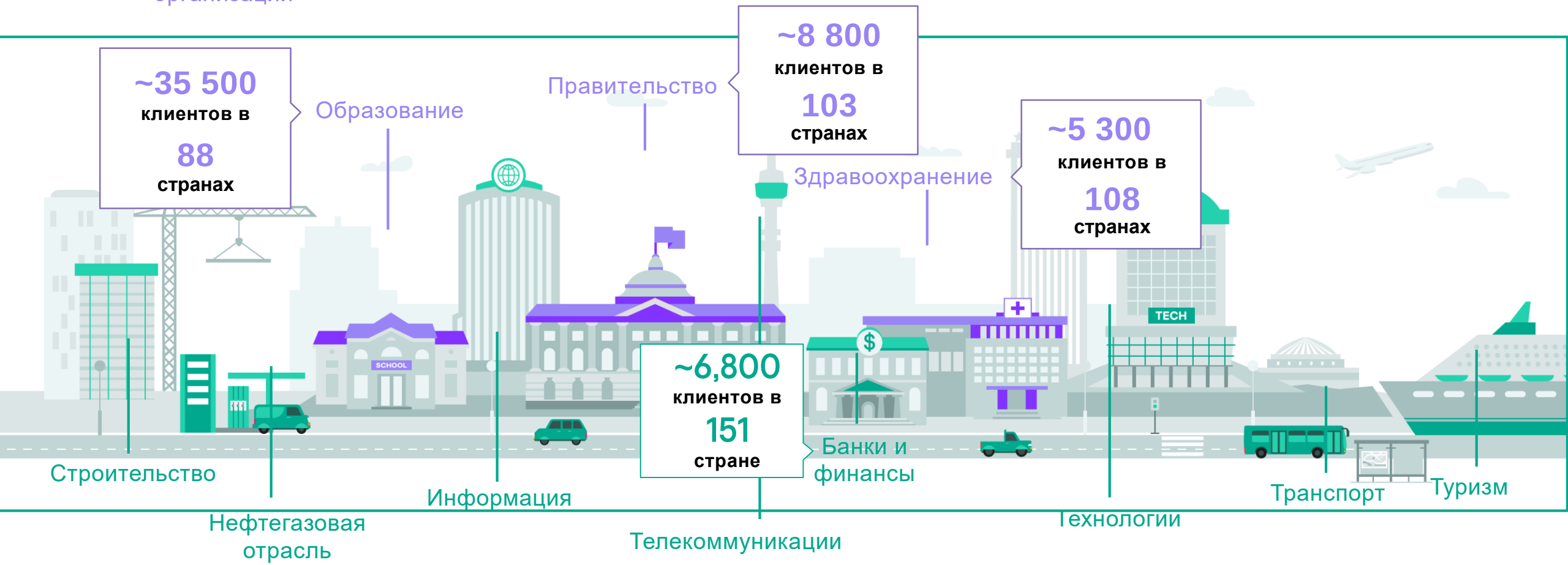
*Canalys Cybersecurity Global Vendor Benchmark report, 2020.

Наши клиенты

Мы работаем в разных секторах экономики.
Наши решения и сервисы успешно защищают более 240 тысяч корпоративных клиентов по всему миру вне зависимости от их размера или сферы деятельности.

● Государственные организации

● Частные компании



Технологические и OEM-партнеры

~120 лидеров индустрии доверяют нам защиту своих клиентов

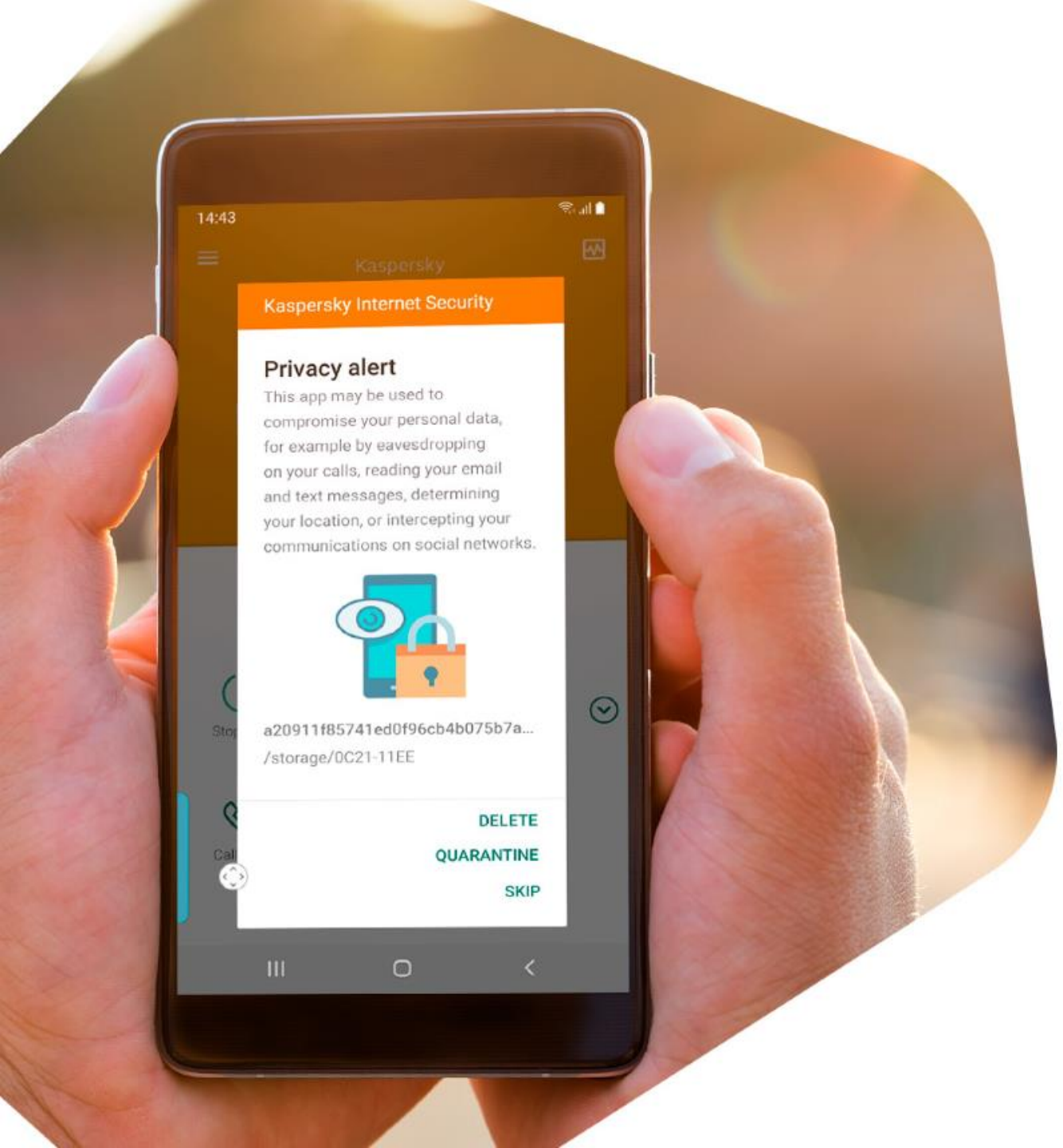
- Интеграция технологий
- Собственные марки/ Кобрендинг
- Предустановка / Набор продуктов
- Предзагрузка

Корпоративная социальная ответственность

Мы строим безопасное будущее, и мы заинтересованы не только в цифровой сохранности мира.

Мы поддерживаем волонтерские и социальные проекты в различных регионах и для этого сотрудничаем с некоммерческими организациями и запускаем собственные инициативы.

Отчет о корпоративной социальной ответственности находится по ссылке: https://csr.kaspersky.com/index.html.



Коалиция по борьбе со сталкерским ПО

«Лаборатория Касперского» находится на переднем краю защиты жертв сталкерского ПО.

С апреля 2019 года в решении Kaspersky Internet Security for Android существует отдельная функция, с помощью которой продукт предупреждает пользователей, если обнаруживает на устройстве программу для слежки. Функция называется Privacy Alert. Для ее создания мы скооперировались с Фондом Электронных Рубежей.

В 2019 году «Лаборатория Касперского» объединилась с 9 другими организациями для создания глобальной инициативы по защите пользователей от слежки через цифровые устройства и домашнего насилия. За первый год существования коалиции число ее участников выросло до 26.

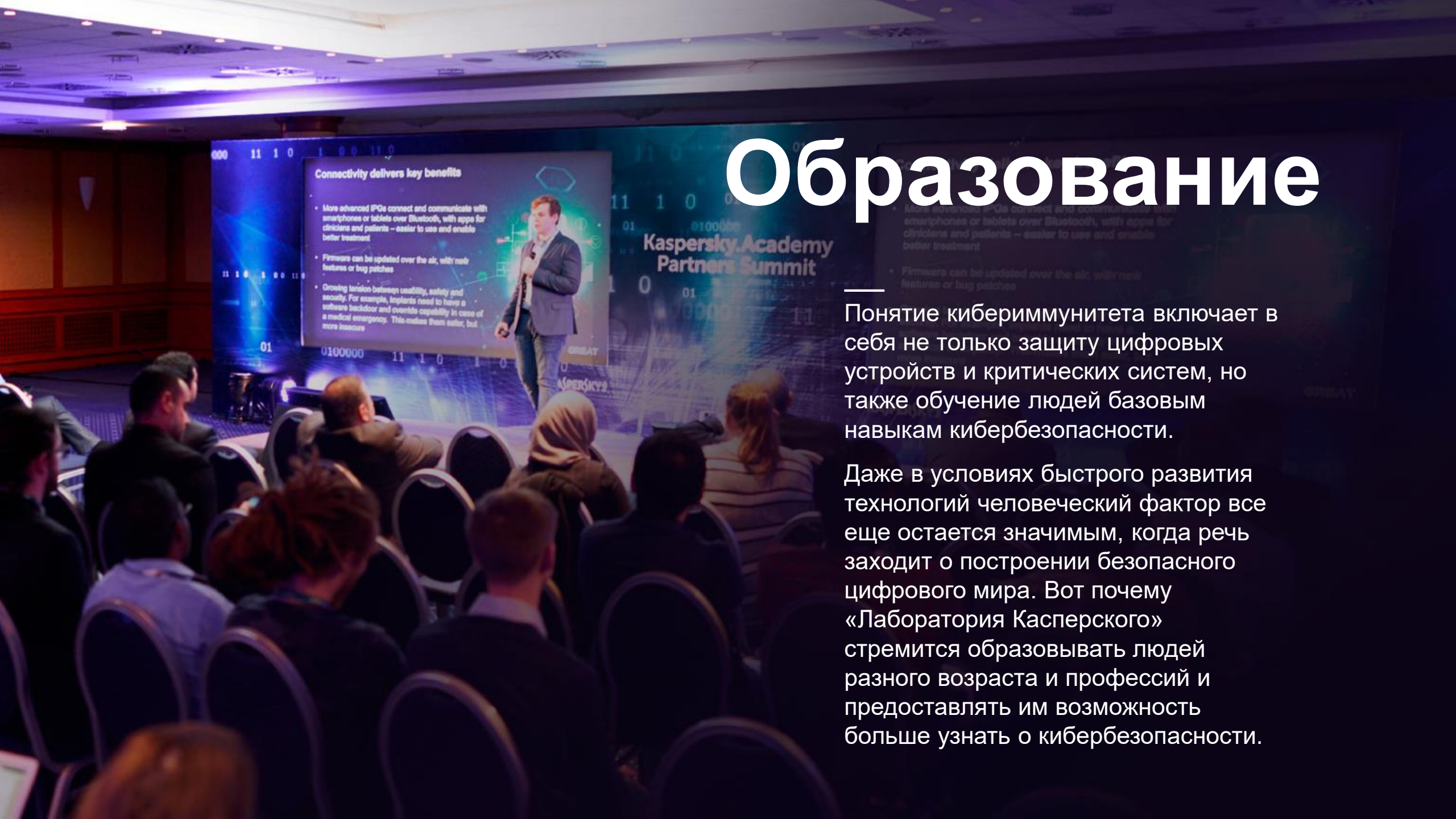
Эксперты команды GReAT разработали утилиту TinyCheck с открытым исходным кодом. Она предназначена для устройств, работающих на платформе Raspberry Pi, и детектирует сталкерское и шпионское ПО.

Сохраняем мир

Мы понимаем важность сохранения культур прошлого для будущих поколений. Вот почему с 2015 года «Лаборатория Касперского» сотрудничает с Афинским археологическим обществом, помогая ему в работе на раскопках Акротири. Цель этого проекта — сохранить руины поселения кикладской/минойской цивилизации на острове Санторини. Этот древний город известен как «греческий Помпеи». Компания является основным спонсором проекта. При ее участии ученые возобновили раскопки и запустили программы по консервации руин и сохранению уникальной настенной живописи.

Сохраняем мир

В июле 2019 года «Лаборатория Касперского» выступила спонсором экспедиции на Курильские острова, которая объединила известных экоактивистов, ученых, фотографов и документалистов. Это путешествие было организовано с целью исследовать уникальную экосистему одного из самых удаленных архипелагов и привлечь внимание общественности к экологическим проблемам, с которыми сегодня сталкиваются Курилы.



Образование

Понятие кибериммунитета включает в себя не только защиту цифровых устройств и критических систем, но также обучение людей базовым навыкам кибербезопасности.

Даже в условиях быстрого развития технологий человеческий фактор все еще остается значимым, когда речь заходит о построении безопасного цифрового мира. Вот почему «Лаборатория Касперского» стремится образовывать людей разного возраста и профессий и предоставлять им возможность больше узнать о кибербезопасности.

Школы

С 2018 года «Лаборатория Касперского» ведет собственный образовательный курс для школьников с акцентом на программирование и информационную безопасность. Проект, получивший название «Математическая вертикаль Касперского», реализован на базе московской школы 1409 и охватывает учеников 7-10 классов.

В рамках сотрудничества с издательствами «Бином» и «Просвещение» эксперты компании приняли участие в подготовке ряда учебных пособий по информатике для российских школьников.

Университеты

В рамках международного образовательного проекта Kaspersky.Academy мы стремимся распространять знания в области кибербезопасности среди студентов по всему миру.

Также «Лаборатория Касперского» поддерживает интерес молодых талантов к сфере IT и кибербезопасности с помощью ежегодного конкурса студенческих проектов Secur’IT Cup.

Бизнес

Мы видим, что бизнес все больше волнуют вопросы кибербезопасности, и мы рады поделиться своими знаниями и опытом с топ-менеджерами компаний из самых различных отраслей. С этой целью «Лаборатория Касперского» сотрудничает с бизнес-школами. Так, в INSEAD — одном из трех ведущих учебных заведений в сфере обучения руководящих работников и подготовке по программам MBA — эксперты компании читают лекции о кибербезопасности.

В рамках проекта Kaspersky.Academy мы предлагаем слушателям программ MBA тренинги по информационной безопасности и организационным политикам.

Школы

С 2018 года «Лаборатория Касперского» ведет свой собственный образовательный курс для школьников с акцентом на программирование и информационную безопасность. Проект, получивший название «Математическая вертикаль Касперского», реализован на базе московской школы 1409 и охватывает учеников 7-10 классов.

В рамках сотрудничества с издательствами «Бином» и «Просвещение» эксперты компании приняли участие в подготовке учебников по информатике для российских школьников 7 и 9 классов, а также специального учебного пособия по информационной безопасности.

Университеты

В рамках своего международного образовательного проекта Kaspersky.Academy мы стремимся распространять знания в области кибербезопасности среди студентов по всему миру.

Также «Лаборатория Касперского» поддерживает интерес молодых талантов к сфере IT и кибербезопасности с помощью ежегодного конкурса студенческих проектов Secur’IT Cup.

Бизнес

Мы видим, что бизнес все больше волнуют вопросы кибербезопасности, и мы рады поделиться своими знаниями и опытом с топ-менеджерами компаний из самых различных отраслей. С этой целью «Лаборатория Касперского» сотрудничает с бизнес-школами. Так, в INSEAD — одном из трех ведущих учебных заведений в сфере обучения руководящих работников и подготовки по программам MBA — эксперты компании читают лекции о кибербезопасности.

В рамках проекта Kaspersky.Academy мы предлагаем слушателям программ MBA тренинги по информационной безопасности и разработке соответствующих политик в организации.

Фото: Maxence Torilloux для INSEAD

Спонсорства и партнерства

Как международная инновационная компания, мы думаем о будущем, не только предоставляя киберзащиту различным отраслям, но также поддерживая перспективные проекты и талантливых людей в разных странах мира.

Мы помогаем развивать науку и современное искусство, поддерживаем культурные проекты и даем спортсменам возможность реализовать свой потенциал по максимуму.

Спорт

У нас долгосрочное партнерство с командой Scuderia Ferrari в гонках «Формулы-1» и футбольным клубом Eintracht Frankfurt. В 2021 году мы стали спонсором Aprilia Racing. Компания поддерживает талантливых пилотов в разных гоночных сериях. Среди них Джанкарло Физикелла, Антонио Джовинацци, Джулиано Алези, Антонио Фуоко, Амна и Хамда Аль Кубаиси.

Наука и космос

Компания поддерживает Starmus — один из самых амбициозных научных и музыкальных фестивалей в мире. Кроме того, «Лаборатория Касперского» выступает стратегическим партнером научно-исследовательского испытательного центра подготовки космонавтов имени Ю.А. Гагарина — в этом центре в Звездном Городке космонавты со всего мира тренируются перед полетом в космос.

Шахматы

«Лаборатория Касперского» является официальным партнером в сфере кибербезопасности для серии престижных шахматных турниров FIDE World Championship, а также обеспечивает комплексную защиту гейминг-платформы FIDE Online Arena от киберугроз.
Компания также поддерживает молодых шахматистов, в том числе Динару Садуакасову и Андрея Цветкова.

Искусство

«Лаборатория Касперского» является партнером международной выставки современного искусства в Лондоне Moniker International Art Fair и поддерживает специальные проекты известных во всем мире художников, например Бена Айне. Кроме того, компания участвовала в реализации креативных проектов совместно с известными стрит-арт художниками D*Face, SHOCK-1 и Фелипе Пантоне.

Спорт

У нас долгосрочное партнерство с командой Scuderia Ferrari в гонках «Формулы-1» и футбольным клубом Eintracht Frankfurt.

В 2021 году мы стали спонсором Aprilia Racing — одного из самых успешных брендов в истории мотогонок.

Помимо этого, мы поддерживаем талантливых пилотов из других гоночных серий. Среди них Джанкарло Физикелла, Антонио Джовинацци, Джулиано Алези, Антонио Фуоко, Амна и Хамда Аль Кубаиси.

Шахматы

«Лаборатория Касперского» является официальным партнером в сфере кибербезопасности для серии престижных шахматных турниров FIDE World Championship, а также обеспечивает комплексную защиту гейминг-платформы FIDE Online Arena от киберугроз.

Компания также поддерживает молодых шахматистов, в том числе Динару Садуакасову и Андрея Цветкова.

Наука и космос

Компания поддерживает Starmus — один из самых амбициозных научных и музыкальных фестивалей в мире. Кроме того, «Лаборатория Касперского» выступает стратегическим партнером научно-исследовательского испытательного центра подготовки космонавтов имени Ю.А. Гагарина — в этом центре в Звездном Городке космонавты со всего мира тренируются перед полетом в космос.

Искусство

«Лаборатория Касперского» является партнером международной выставки современного искусства в Лондоне Moniker International Art Fair и поддерживает специальные проекты известных во всем мире художников, например Бена Айне. Кроме того, компания реализовала креативный проект совместно с британским стрит-арт художником D*Face. А в рамках сотрудничества с другим британским художником, SHOK-1, известным всему миру своими граффити, которые напоминают рентгеновские снимки, компания представила арт-рентген своего талисмана — зеленого медведя Мидори Кума. В 2021 году «Лаборатория Касперского» создала коллаборацию с современным художником Фелипе Пантоне с целью повысить осведомленность широкой аудитории в вопросах приватности в День защиты данных.

Активируй будущее

kaspersky