О «Лаборатории Касперского»

kaspersky

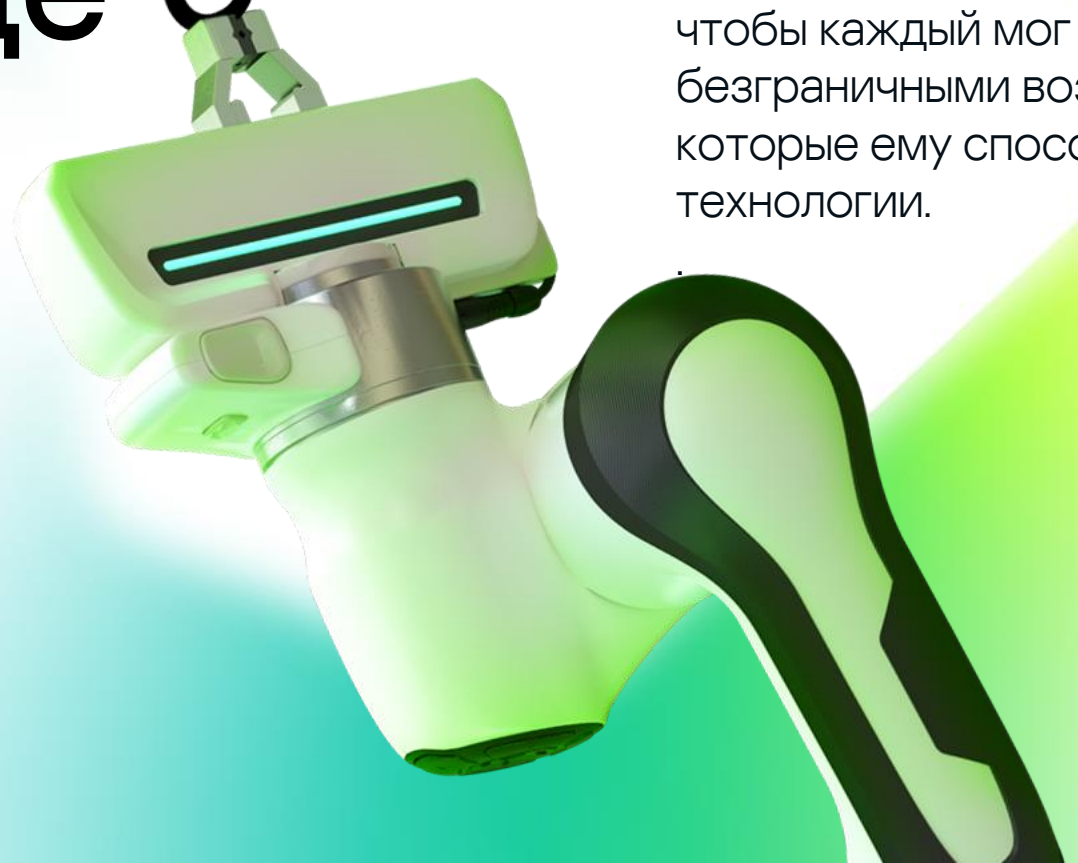
Ноябрь 2022

У нас простая и понятная миссия — мы строим безопасный мир

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

Евгений Касперский,
генеральный директор

Активируй будуще е



Мы верим, что в будущем технологии помогут улучшить жизнь всего человечества. Вот почему мы стремимся обеспечить их безопасность — чтобы каждый мог наслаждаться теми безграничными возможностями, которые ему способны предложить технологии.

«Лаборатория Касперского»

- Ключевые факты
- Клиенты
- География
- Роль в международном ИБ-сообществе

Ключевые факты

Основное

Основана в 1997 году, возглавляется Евгением Касперским

Работает на 6 континентах почти в 200 странах и территориях мира

Разрабатывает инновационные IT-решения для защиты корпоративных и домашних пользователей

Цифры

> 15 млн
активаций в год

Почти 5 000
высококвалифицированных специалистов

752 млн долларов
— глобальная аудированная выручка в 2021 году

Клиенты

Наши решения и сервисы защищают самых разных клиентов: от домашних пользователей до компаний разных масштабов, а также крупные предприятия, объекты критической инфраструктуры и государственные органы

>240 тысяч

корпоративных клиентов по всему миру

>400 млн

пользователей по всему миру защищены нашими технологиями

Крупный бизнес

Промышленные предприятия

Небольшие компании

Микробизнес

Домашние пользователи

Клиенты

Мы работаем в разных секторах экономики. Наши решения и сервисы успешно защищают более 240 тысяч корпоративных клиентов по всему миру

200 стран и территорий

34 региональных офиса

Африка
Южная Африка

Азия
Китай
Гонконг
Индия
Япония
Казахстан
Малайзия
Сингапур
Южная Корея

Европа
Чехия
Франция
Германия
Израиль
Италия
Нидерланды
Португалия
Румыния
Россия
Испания
Швейцария
Великобритания

Ближний Восток
Саудовская Аравия
Турция
ОАЭ

Северная Америка
Мексика
США

Южная Америка
Бразилия

Центры прозрачности
Цюрих, Швейцария
Мадрид, Испания
Сан-Паулу, Бразилия
Куала-Лумпур, Малайзия
Вобурн, США
Сингапур, Сингапур
Токио, Япония
Рим, Италия
Утрехт, Нидерланды

Наша роль в мировом сообществе по информационной безопасности

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

INTERPOL

Coalition Against Stalkerware

PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE
11 • 12 • 2018

industrial internet CONSORTIUM

Глобальная инициатива по информационной открытости

- Ключевые принципы прозрачности
- Глобальная инициатива по информационной открытости
- Независимые тесты и сертификаты
- Программа Bug Bounty

Наши принципы прозрачности ведения бизнеса

Данные, которые мы получаем от пользователей, анонимизированы и защищены. Мы понимаем, насколько это важно для безопасности пользователей

Мы обнаруживаем и нейтрализуем все виды киберугроз независимо от их цели или происхождения

В деле борьбы с киберзлом мы объединяем усилия с международными организациями

Мы придерживаемся принципов защищенной разработки при создании технологий и решений

Мы сотрудничаем с ИБ-сообществом и совместно расследуем киберпреступления

Глобальная инициатива по информационной открытости

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

Инициатива предусматривает ряд конкретных мер и шагов:

Перенос в Швейцарию инфраструктуры по обработке и хранению данных пользователей

Создание глобальной сети Центров прозрачности, где партнеры и клиенты могут получить информацию о программном коде продуктов компании, их обновлениях, антивирусных базах, правилах распознавания угроз

Независимая оценка процесса безопасной разработки и стратегии по минимизации рисков в цепочке поставок и в программном обеспечении

Глобальная инициатива по информационной открытости

Инициатива предусматривает ряд конкретных мер и шагов:

Программа Bug Bounty, которая предусматривает вознаграждение за обнаружение уязвимостей в ПО «Лаборатории Касперского»

Публичные отчеты, в которых мы делимся информацией о числе запросов о данных пользователей и запросов технической информации

Запуск обучающей программы Cyber Capacity Building Program, которая позволяет получить навыки оценки уровня безопасности IT-инфраструктуры

Глобальная инициатива по информационной открытости

Перенос инфраструктуры по обработке и хранению данных пользователей

Вредоносные и подозрительные файлы, получаемые от пользователей продуктов «Лаборатории Касперского» из Европы, США, Канады, Латинской Америки, Ближнего Востока и некоторых стран Азиатско-Тихоокеанского региона, обрабатываются и хранятся на серверах в Швейцарии.

Центры прозрачности

В них партнеры и клиенты компании могут получить информацию о программном коде продуктов «Лаборатории Касперского», их обновлениях, правилах распознавания угроз.

Независимый обзор

Регулярная сторонняя оценка внутренних процессов для подтверждения безопасности процессов и систем компании, в том числе:

- Аудит SOC 2, проведенный одной из компаний «Большой четверки».
- Сертификация ISO 27001.

Программа Bug Bounty

Увеличение размера вознаграждения в программе bug bounty до 100 тысяч долларов США за обнаружение наиболее серьезных уязвимостей в ПО «Лаборатории Касперского».

Публикация отчетов с данными о внешних запросах

Регулярные отчеты о том, как «Лаборатория Касперского» работает с запросами от государственных структур, правоохранительных органов и обычных пользователей.

Центры прозрачности

Возможности:

Blue Piste (и удалённо, и физически)

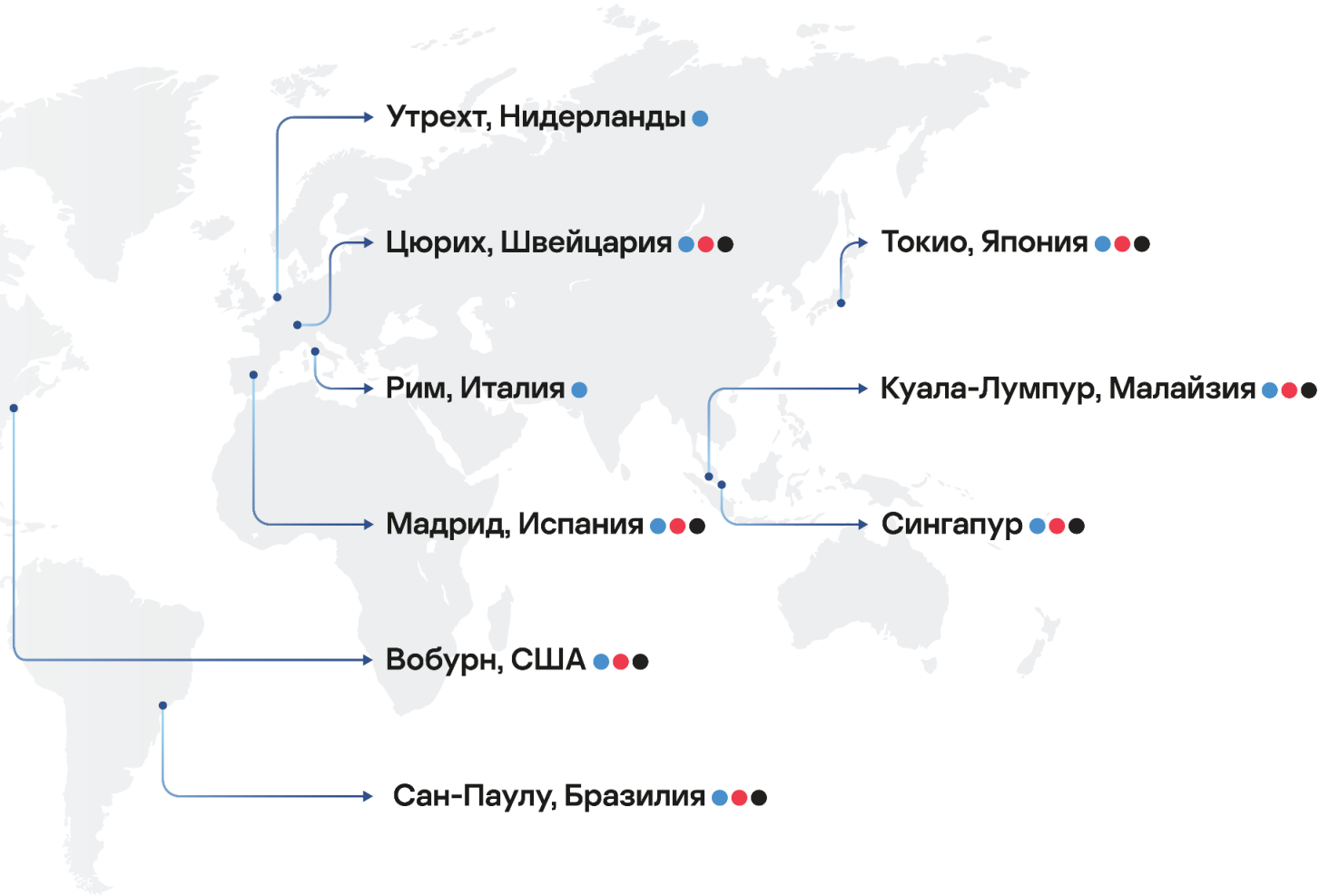
Обзор практик прозрачности, продуктов и сервисов компании, а также практик управления данными.

Red Piste

Обзор наиболее критичных частей исходного кода с помощью экспертов компании.

Black Piste

Наиболее глубокий обзор самых критичных частей исходного кода с помощью экспертов компании.



Глобальная инициатива по информационной открытости: результаты в цифрах

2 дата-центра

в Швейцарии, известной во всем мире как нейтральная страна. В ней строго регулируются вопросы защиты данных.

В них мы обрабатываем и храним данные пользователей из Европы, Северной и Латинской Америки, Ближнего Востока и некоторых стран Азиатско-Тихоокеанского региона.

9 Центров прозрачности

в Бразилии, Италии, Японии, Малайзии, Нидерландах, Сингапуре, Испании, Швейцарии и США.

2 регулярных сторонних независимых оценки

Они подтверждают надежность принятых в компании практик разработки:

- Аудит SOC 2, проведенный одной из компаний «Большой четверки».
- Сертификация ISO 27001.

30+ посещений Центров прозрачности

представителями частных и государственных компаний. Эксперты «Лаборатории Касперского» в том числе два раза провели обзор наиболее критичных частей исходного кода.

53 участника программы Bug Bounty получили вознаграждение

Общий размер выплат составил более 75 тысяч долларов США.

Сертификация

SOC

Всемирно признанный стандарт отчета для системы управления рисками кибербезопасности. Разработан Американским институтом дипломированных бухгалтеров (American Institute of Certified Public Accountants, AICPA). «Лаборатория Касперского» успешно прошла аудит SOC 2 в 2022 году.

ISO/IEC 27001

Международный стандарт систем менеджмента информационной безопасности. Вбирает в себя лучшие мировые практики управления информационной безопасностью. «Лаборатория Касперского» успешно прошла аудит ISO/IEC 27001:2013.

Программа Bug Bounty

«Лаборатория Касперского» придерживается принципов этического раскрытия уязвимостей. Она реализует свою программу bug bounty с 2016 года. Компания также поддерживает проект Disclose.io, который является «безопасной гаванью» (Safe Harbor) для исследователей уязвимостей, обеспокоенных возможными негативными юридическими последствиями своих открытий.

Вознаграждение

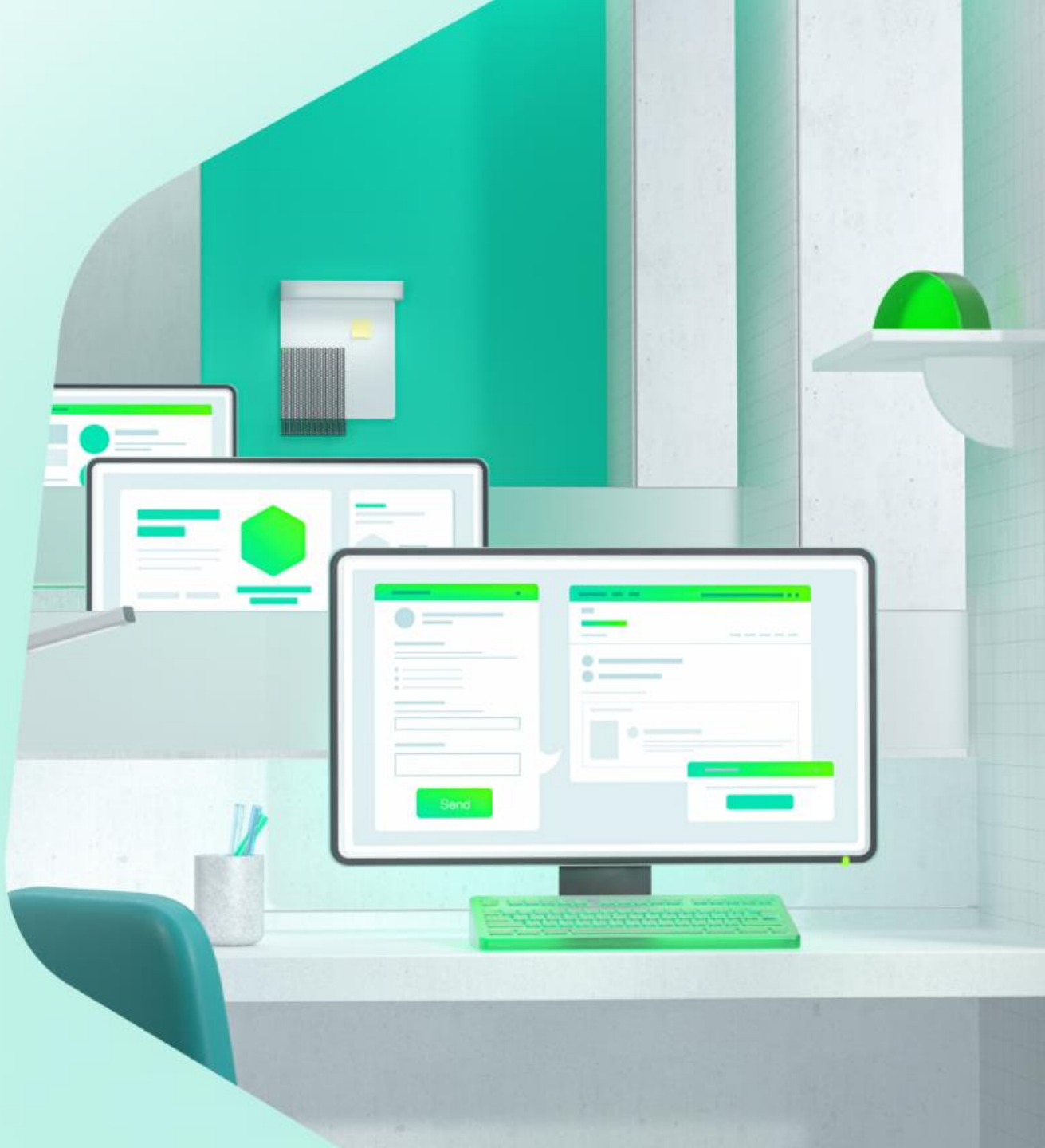
$100,000
за обнаружение и ответственное раскрытие наиболее серьезных уязвимостей

$5,000 – $20,000
за обнаружение уязвимостей, позволяющих реализовать менее серьезные варианты удалённого выполнения кода

$1,000 – $5,000
за обнаружение брешей в ПО, позволяющих повысить локальные права доступа или приводящих к раскрытию конфиденциальных данных

Аналитика угроз и исследования

- Эксперты
- Исследование угроз
- Ландшафт сложных угроз
- Ключевые открытия и исследования
- Исследование целевых атак
- Вклад в обеспечение приватности



Эксперты

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

Почти 5 000 высококвалифицированных специалистов

50% наших сотрудников — R&D-специалисты

35+ ведущих мировых экспертов в области кибербезопасности

Исследование угроз

Более млрд

киберугроз

обнаружила «Лаборатория Касперского» с момента своего основания

8 млрд

кибератак

обнаружила «Лаборатория Касперского» в 2021 году

380 тысяч

новых вредоносных файлов

обнаруживает «Лаборатория Касперского» ежедневно

Ландшафт сложных угроз в 2021 году

В «Лаборатории Касперского» создан Глобальный центр исследований и анализа угроз. Он известен во всем мире благодаря расследованиям наиболее сложных кибератак. Согласно данным этого центра, в 2021 году главной мишенью сложных и хорошо спланированных кибероперации стали правительственные органы, а наиболее активной группировкой оказалась Lazarus.

10 наиболее атакуемых отраслей

- Госорганы
- Дипломатия
- Телеком
- Вооруженные силы
- ОПК
- IT-компании
- Образование
- Гражданская авиация
- Логистика
- Фармацевтика

10 наиболее опасных кибергрупп

1. Lazarus
2. DarkHalo
3. CloudComputating
4. Turla
5. SideCopy
6. MuddyWater
7. APT41
8. BlueNoroff
9. HoneyMyte
10. Gamaredon

Топ-12 атакованных стран

Данные от 31.12.2021

apt.securelist.com

Наши главные расследования и открытия

	Sofacy	Duqu 2.0	Lazarus	Project Sauron	Expetr/ Notpetya	Shadowpad	Olympic destroyer	Shadow hammer	Tajmahal	Mosaic-regressor	Ghostemperor
Обнаружение	2014	2015	2016	2016	2017	2017	2018	2018	2019	2020	2021
Начало активности	2008	2014	2009	2011	2017	2017	2017	2018	2013	2017	2020
Классификация	ПО для кибершпионажа	Комплексная платформа для кибератак	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	ПО для кибершпионажа
Цели	Военные и государственные организации по всему миру	Заражениям подверглись площадки, на которых проходили высокопоставленные встречи мировых лидеров группы P5+1	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 строительство, производство и другие отрасли	Организации, имеющие отношение к Зимним Олимпийским играм 2018; европейские организации, изучающие биологические и химические угрозы; финансовые организации в России	Банковские и финансовые учреждения, ПО, СМИ, энергетика и коммунальное хозяйство, страхование, промышленность и строительство, производство и другие отрасли	Специальные инструкции во вредоносном коде устанавливали в качестве цели 600 систем, определённых по специальным, MAC-адресам	Дипломатические представительства, чья деятельность связана с Северной Кореей	Правительственные организации и телекоммуникационные компании

Целевые атаки: хронология расследований

2016

- ProjectSauron
- StrongPity
- Lazarus
- Fruity Armor
- ScarCruft
- Poseidon
- Danti
- Dropping Elephant

2017

- WannaCry
- Shamoon 2.0
- StoneDrill
- BlueNoroff
- ExPetr/NotPetya
- Moonlight Maze
- ShadowPad
- BlackOasis
- Silence
- WhiteBear

2018

- Zebrocy
- DarkTequila
- MuddyWater
- Skygofree
- Olympic Destroyer
- ZooPark
- Hades
- Octopus
- AppleJeus

2019

- Topinambour
- ShadowHammer
- SneakyPastes
- FinSpy
- DarkUniverse
- COMpfun
- Titanium

2020

- Cycldek
- SixLittleMonkeys (aka Microcin)
- CactusPete
- DeathStalker
- MATA
- TransparentTribe
- WellMess
- TwoSail Junk
- MontysThree
- MosaicRegressor
- VHD Ransomware
- WildPressure
- PhantomLance

2021

- GhostEmperor
- ExCone
- BlackShadow
- BountyGlad
- EdwardsPhesant
- HotCousin
- GoldenJackal
- FerociousKitten
- ReconHellcat
- CoughingDown
- MysterySnail
- CraneLand

Вклад в обеспечение приватности

Вопросы приватности в цифровом пространстве становятся все более актуальными. Все больше людей стремятся изменить свои привычки, чтобы сделать свое присутствие в сети более защищенным. Как компания, работающая в сфере не только информационной безопасности, но и цифровой приватности, «Лаборатория Касперского» разрабатывает инструменты для защиты приватности и курсы для повышения цифровой грамотности.

Курс по доксингу

В курсе рассказывается, что это за угроза и как ее избежать

https://go.kaspersky.com/doxing-course

Защита от сталкерского ПО

Kaspersky Internet Security для Android предлагает лучшие в своем классе защиту и возможности детектировать ПО для тайной слежки

https://stopstalkerware.org/ru/

Privacy Checker

Сайт с инструкциями по настройкам приватности в социальных сетях, браузерах, операционных системах

https://privacy.kaspersky.com/ru/

Продукты и решения

- Кибериммунный подход
- KasperskyOS
- B2B-решения
- Решения для защиты промышленных сред
- Решения для защиты малого и среднего бизнеса
- MSP-решения
- B2C-решения

От кибербезопасности к кибериммунитету

Традиционный подход (кибербезопасность)

Бесконечная гонка: поиск и закрытие уязвимостей

Вирус/антивирус, фишинг в электронной почте/защита электронной почты

Врожденная безопасность (кибериммунность)

Определяется целями продукта и безопасности

Микроядро, изолированные домены, политики безопасности

KasperskyOS

Архитектурный подход создает среду, в которой уязвимость или ошибка в коде больше не представляет опасности.

- IT-системы с врожденной безопасностью — это системы, которые могут противостоять кибератакам без дополнительных средств защиты
- Уникальная методология для создания IT-систем с врожденной защитой
- Платформа для создания кибериммунных IT-систем – KasperskyOS, собственная микроядерная операционная система компании для IT-продуктов с высокими требованиями к кибербезопасности

Сферы применения

Решения на базе KasperskyOS обладают встроенной защищенностью от подавляющего большинства видов кибератак.

Они способны выполнять свои критические функции даже в агрессивной среде, без дополнительных средств защиты.

Интернет вещей и промышленный интернет вещей

Контроллеры для умных городов

Виртуальные рабочие столы

Транспорт

Корпоративные мобильные устройства

Доверенные среды исполнения

Портфолио продуктов на базе KasperskyOS

Kaspersky IoT Infrastructure Security

Решение для защиты устройств интернета вещей, которое можно подключать к облакам, с безопасными шлюзами в качестве ключевых элементов

Kaspersky IoT Secure Gateway

KISG 100

На платформе Siemens SIMATIC IOT2040

KISG 1000

На платформе Advantech UTX-3117

Kaspersky Security Center

Kaspersky Secure Remote Workspace

Решение для построения управляемой и функциональной инфраструктуры тонких клиентов, а также централизованного управления ей

Kaspersky Thin Client

Kaspersky Security Center

Kaspersky Security Management Suite

Powered by KasperskyOS

B2B-решения

Специализированные решения

- Kaspersky Industrial CyberSecurity
- Kaspersky Fraud Prevention
- Kaspersky Research Sandbox
- Kaspersky Threat Attribution Engine
- Kaspersky Private Security Network

Уровень 3
Сложные целевые атаки

Expert Security
Зрелая служба ИБ или SOC

- Тренинги для ИБ-специалистов: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky Endpoint Detection and Response Expert; Kaspersky Anti Targeted Attack
- Оценка: Kaspersky Security Assessment
- Внешние эксперты: Kaspersky Incident Response
- Обучение цифровой грамотности: Kaspersky Security Awareness Ultimate

Уровень 2
Трудно обнаруживаемые угрозы

Optimum Security
Команда ИБ

- Обучение цифровой грамотности: Kaspersky Security Awareness Advanced
- Прозрачность и реагирование: Kaspersky Endpoint Detection and Response Optimum
- Обогащение данными: Kaspersky Threat Intelligence Portal

Уровень 1
Массовые угрозы

Security Foundations
IT

- Конечные устройства: Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security; Kaspersky Hybrid Cloud Security
- Сеть: Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway
- Данные: Kaspersky Security for Storage
- Обучение цифровой грамотности: Kaspersky Security Awareness Essential
- Поддержка: Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

Kaspersky Industrial Cybersecurity Solution

Kaspersky Industrial CyberSecurity

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

Kaspersky ICS CERT

Экспертные сервисы и консультационные услуги

Продукты

- **Защищенный промышленный шлюз**
  - Kaspersky IoT Secure Gateway
- **Защита промышленных конечных устройств**
  - KICS for Nodes
- **Обнаружение аномалий и утечек в промышленной сети**
  - Kaspersky Machine Learning for Anomaly Detection
  - KICS for Networks
- **Централизованное управление безопасностью**
  - Kaspersky Security Center

Сервисы

- **Цифровая грамотность**
  - Kaspersky Security Awareness
  - Kaspersky Security Trainings
- **Экспертные сервисы и аналитика угроз**
  - Kaspersky Security Assessment
  - Kaspersky Incident Response
  - Kaspersky Threat Intelligence

В числе поддерживаемых устройств и протоколов

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

Решения нового поколения для малого и среднего бизнеса

Kaspersky Small Office Security

Легкий в управлении, как и домашний антивирус

- Готовое решение, дополнительные настройки не требуются
- Защита от финансового мошенничества с Safe Money
- Защита клиентских и личных данных. Шифрование и резервное копирование данных.
- Хранение паролей в Password Manager

Kaspersky Endpoint Security Cloud

Быстрая защита в условиях ограниченных ресурсов

- Облачная консоль для гибкого и простого управления, нет необходимости покупать дополнительное оборудование
- Защита ПК, файловых серверов, ноутбуков и мобильных устройств
- Защита Microsoft Office 365 и контроль теневых ресурсов
- Новейшее, наиболее современное ПО

Kaspersky Optimum Security

Защита уровня корпораций

- Основная EDR-функциональность для борьбы с трудно обнаруживаемыми угрозами
- Управляемая защита выводит безопасность на новый уровень
- Снижает нагрузку на ИБ-специалистов
- Облачное решение, которое защищает разные среды и платформы

Сервисы для поставщиков управляемых услуг

- Защита конечных устройств
- Управление уязвимостями и патчами
- Защита Office365

- Реагирование на инциденты
- Тренинги
- Управляемая защита веб- и почтовых ресурсов

- Круглосуточный мониторинг безопасности
- Детектирование и реагирование
- Проактивный поиск угроз

MSP

- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365
- Kaspersky EDR Optimum
- Kaspersky Hybrid Cloud Security
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway

MSSP

- Kaspersky EDR Expert
- Kaspersky Anti Targeted Attack
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky Intelligence Reporting

\+ Kaspersky Managed Detection and Response

Автоматизация и интеграция

- Интеграция RMM с PSA
- По подписке и по локальной маржинальной цене

Опыт и знания

- Kaspersky Cybersecurity Training
- Kaspersky Premium Support and Professional Services

B2C-решения

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

Kaspersky B2C Solutions

Kaspersky Who Calls
Android | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Total Security
Win | Android | Mac | iOS

Kaspersky QR Scanner
Android | iOS

Kaspersky Battery Life
Android

Kaspersky Security Cloud
Win | Android | iOS

Kaspersky Internet Security
Win | Android | Mac | iOS

Награды

- Обзор
- Метрика топ-3

Более 600 наград

Входит в пятерку крупнейших вендоров в области защиты конечных устройств*.

Kaspersky Internet Security — **продукт года 2020** по версии независимой тестовой лаборатории AV-Comparatives**.

* Компания заняла пятое место в рейтинге IDC 'Worldwide Consumer Endpoint Security Market Shares, 2020: The COVID-19 Pandemic Contributed to a Market Surge' (Doc #US47714321 / June 2021) и девятое в рейтинге 'Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth' (Doc #US47768021 / June 2021).

** Флагманское решение «Лаборатории Касперского» для домашних пользователей – Kaspersky Internet Security – в 2020 году получило награду Продукт года в шестой раз. Это ежегодный отчет независимой лаборатории AV-Comparatives. Оно превзошло 16 конкурирующих продуктов и получило награды Advanced+ во всех семи тестах годового цикла, показав максимальные результаты в каждом из них.

Признание

Больше тестов*
Больше наград*
Больше защиты

Kaspersky.ru/top3

75
тестов/
обзоров

57
первых мест

Кибербезопасность сегодня жизненно необходима как отдельному человеку, так и целым организациям. 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 2021 году решения «Лаборатории Касперского» участвовали в 75 независимых тестах и обзорах. В 57 из них наши продукты заняли первые места, а в 63 случаях оказались в тройке лидеров.

84%
в 84% случаев заняли одно из трех первых мест

ESG

Мы строим безопасное будущее
и заинтересованы не только в цифровой сохранности мира. Нас волнуют гендерное равенство, доступность знаний, волонтерство, детская безопасность, защита животных и другие вопросы.

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 за 2019-2020 гг. находится здесь.

ESG

Сохранение культуры

Мы понимаем важность сохранения культур прошлого для будущих поколений. С 2015 года «Лаборатория Касперского» сотрудничает с Афинским археологическим обществом

Борьба со сталкерским ПО

«Лаборатория Касперского» и еще более 40 компаний из индустрии кибербезопасности и некоммерческого сектора поддерживают коалицию по борьбе со сталкерским ПО. Это глобальная инициатива по защите пользователей от слежки через цифровые устройства и домашнего насилия

Мы помогаем преодолеть гендерное неравенство и способствуем прогрессу в этом направлении

ESG

Женщины в IT

Мы помогаем преодолеть гендерное неравенство и способствуем прогрессу в этом направлении

Борьба со сталкерским ПО

«Лаборатория Касперского» и еще более 40 компаний из индустрии кибербезопасности и некоммерческого сектора поддерживают коалицию по борьбе со сталкерским ПО. Это глобальная инициатива по защите пользователей от слежки через цифровые устройства и домашнего насилия

Сохранение культуры

Мы понимаем важность сохранения культур прошлого для будущих поколений. С 2015 года «Лаборатория Касперского» сотрудничает с Афинским археологическим обществом

Образование

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

Несмотря на быстрое развитие технологий, человеческий фактор все еще играет важную роль, когда речь заходит о построении безопасного цифрового мира. Вот почему «Лаборатория Касперского» стремится образовывать людей разного возраста и профессий и рассказывать о кибербезопасности как можно больше.

Образование

Школа

«Лаборатория Касперского» обучает школьников правилам интернет-безопасности, в том числе выпустила учебное пособие и разработала образовательные программы

Университет

В рамках международного образовательного проекта Kaspersky.Academy мы стремимся обучать кибербезопасности студентов по всему миру

Бизнес

«Лаборатория Касперского» сотрудничает с бизнес-школами, обучает информационной безопасности лидеров бизнеса, топ-менеджеров и руководителей высшего звена

Спонсорства и партнерства

Мы заботимся о будущем: не только предоставляем киберзащиту различным отраслям, но и поддерживаем 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.

Спонсорства и партнерства

Мотоспорт

«Лаборатория Касперского» спонсирует Aprilia Racing — один из самых успешных брендов в истории мотогонок

Шахматы

«Лаборатория Касперского» — официальный партнер в сфере кибербезопасности для серии престижных шахматных турниров FIDE World Championship

Наука и космос

«Лаборатория Касперского» много лет поддерживает инициативы в области развития космоса, в том числе проводила тренинг по информационной безопасности для космонавтов

Искусство

«Лаборатория Касперского» — партнер международной выставки современного искусства Moniker International Art Fair в Лондоне — и поддерживает художников, например Бена Айне

Киберспорт

«Лаборатория Касперского» является партнером FACEIT, ведущей игровой платформы для проведения киберспортивных турниров

Активируй будущее