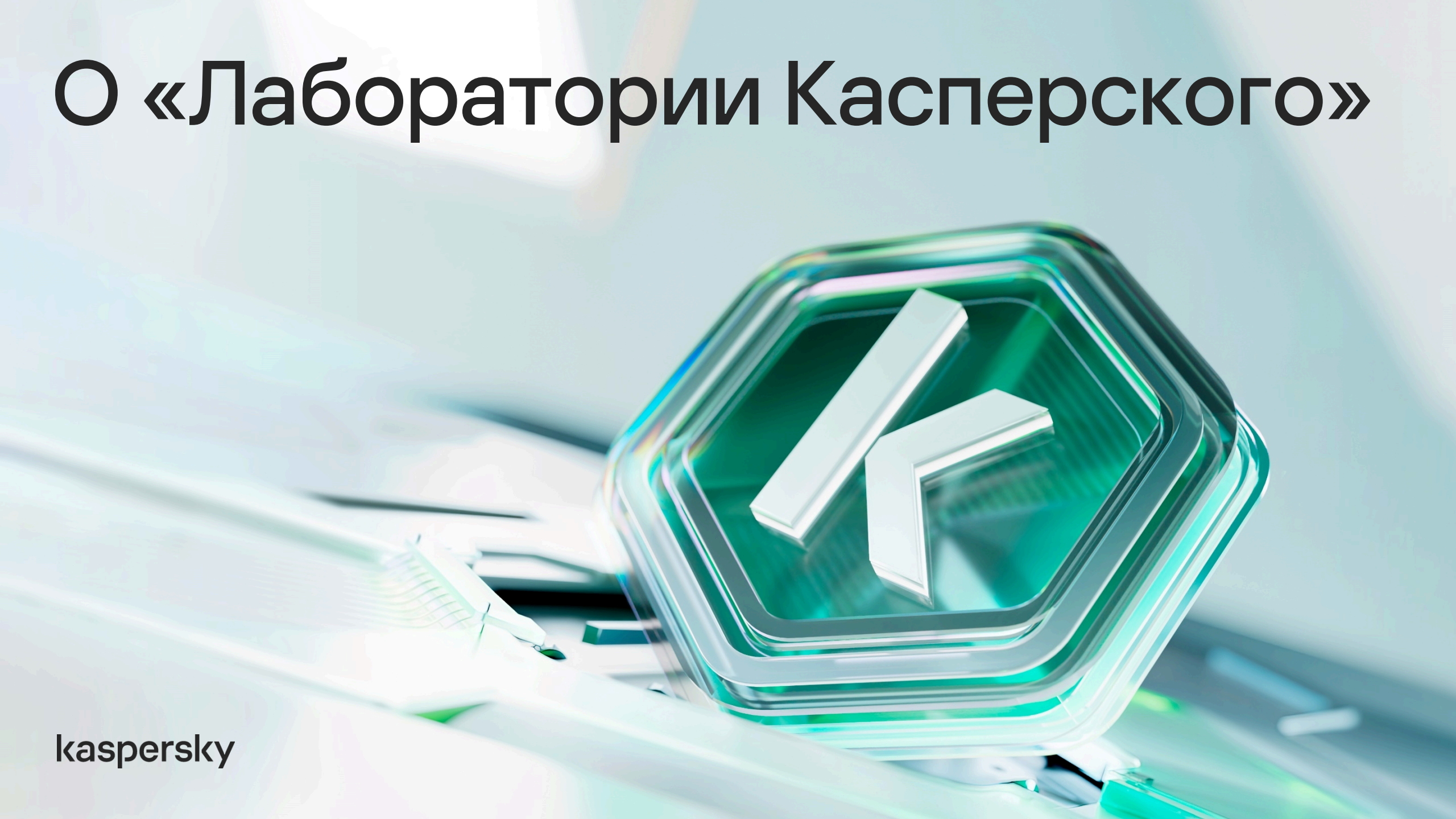
О «Лаборатории Касперского»



kaspersky



У нас простая и понятная миссия — мы строим безопасный мир

Мы делаем это через глобальное лидерство в кибербезопасности. Защищаем цифровое пространство от киберугроз, чтобы каждый получал от технологий только благо.

Активируем бесконечные возможности.
Активируем безопасное будущее.

Евгений Касперский,
генеральный директор «Лаборатории Касперского»

3

О компании

Компания основана в 1997 году, возглавляется Евгением Касперским

Представлена на 5 континентах, в более чем 200 стран и территорий

Разрабатывает инновационные IT-решения и сервисы для защиты корпоративных и частных пользователей

>9 млн

активаций B2C-продуктов в мире в год

> 6 тысяч

специалистов

822 млн долларов США

глобальная выручка в 2024 году

4

Клиенты

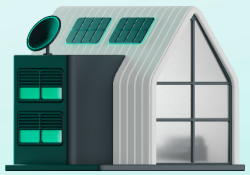
Наши решения и сервисы разработаны, чтобы соответствовать потребностям в кибербезопасности широкого круга заказчиков — от частных пользователей и предприятий малого бизнеса до крупных предприятий, объектов критической инфраструктуры и государственных органов

1 млрд

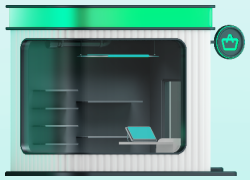
устройств защитила «Лаборатория Касперского»*

около 200 тыс.

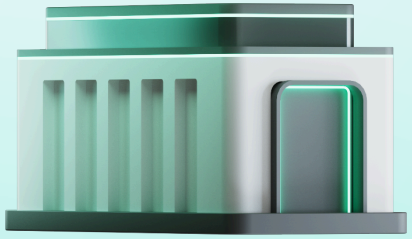
корпоративных клиентов по всему миру находятся под нашей защитой



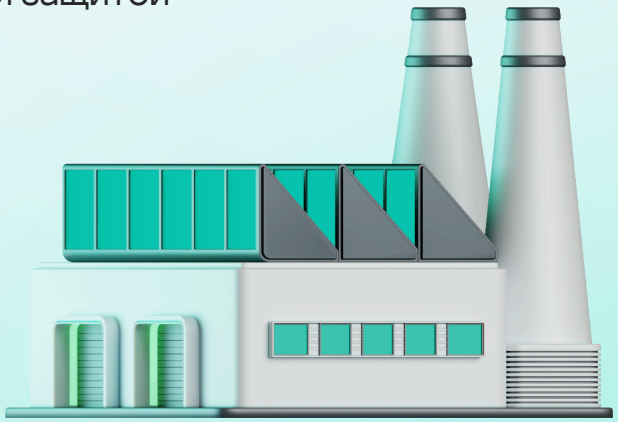
Частные пользователи



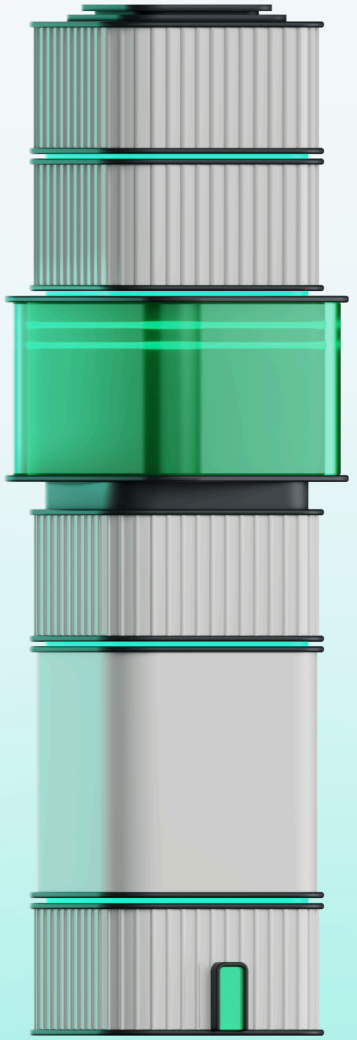
Микробизнес



Малый и средний бизнес



Промышленные предприятия



Крупные корпорации

* Данные с 2011 года, полученные в результате автоматизированного анализа вредоносного ПО с помощью глобальной облачной инфраструктуры Kaspersky Security Network (KSN)

5

Мы международная компания в области кибербезопасности

200 стран и территорий

30+ представительств



Африка
Южная Африка
Кения
Руанда

Азия
Большой Китай (Китай, Гонконг)
Индия
Япония
Казахстан
Малайзия
Сингапур
Южная Корея
Вьетнам

Европа
Беларусь
Чехия
Франция
Германия
Израиль
Италия
Нидерланды
Россия
Испания
Швейцария

Ближний Восток
Саудовская Аравия
Турция
ОАЭ

Латинская Америка
Бразилия
Мексика
Колумбия

Центры прозрачности
Цюрих, Швейцария
Мадрид, Испания
Сан-Паулу, Бразилия
Куала-Лумпур, Малайзия
Кигали, Руанда
Сингапур
Богота, Колумбия
Токио, Япония
Рим, Италия
Утрехт, Нидерланды
Эр-Рияд, Саудовская Аравия
Стамбул, Турция
Сеул, Южная Корея

6

Совместные операции

«Лаборатория Касперского» много лет сотрудничает с Интерполом и Африполом в рамках официальных соглашений, внося свой вклад в совместную работу по противодействию киберпреступности. Компания предоставляет данные о киберугрозах, проводит тренинги и способствует укреплению регионального потенциала для борьбы со злоумышленниками

INTERPOL

AFRIPOL

	Africa Cyber Surge	Africa Cyber Surge II	Synergia	Against Grandoreiro	Serengeti	Олимпиада-2024	Synergia II	Red Card	Secure	Serengeti 2.0
Год	2022	2023	2024	2024	2024	2024	2024	2025	2025	2025
Результаты	Выявление вредоносной инфраструктуры в странах Африки	Арестованы 14 человек, а также выявлена сетевая инфраструктура, использование которой привело к финансовым потери на общую сумму свыше 40 млн долларов США	Нарушение работы инфраструктуры, используемой для фишинговых атак, распространения вредоносного ПО и программ-вымогателей	Арестованы 5 участников кибергруппы, использовавшей в своих атаках банковский троянец Grandoreiro	Арестованы более 1000 подозреваемых в киберпреступлениях, финансовый ущерб от которых составил около 193 млн долларов США	Компания помогла обнаружить фишинговые атаки и другую мошенническую активность во время летних Олимпийских игр во Франции в 2024 году.	Выявлено 100 подозреваемых в 95 странах, из них арестован 41 человек	Арестованы более 300 подозреваемых и остановлена деятельность киберпреступных сетей в семи странах Африки	Выявлена и заблокирована вредоносная активность с использованием программ-стилеров в 26 странах Азиатско-Тихоокеанского региона	Арестованы 1209 подозреваемых
	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее	Подробнее

7

Уникальная команда экспертов

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

>5,5 тыс. специалистов

>50% сотрудников работают в R&D

35+ экспертов в команде Глобального центра исследования и анализа угроз — Kaspersky GReAT



8

Технологическое лидерство, обогащенное глобальным опытом

Исследование угроз
Анализ инцидентов

Expertise Centers

Глобальный центр исследования и анализа угроз

GREAT

Исследование наиболее сложных угроз (APT, кампании кибершпионажа, глобальные киберэпидемии)

Анализ сложного финансового вредоносного ПО

Безопасность инновационных технологий

Центр исследования угроз

Threat Research

Безопасная разработка и конструктивная безопасность

Анализ онлайн-угроз и контентная фильтрация

Исследование угроз от вредоносного ПО до APT, создание детектирующей логики

Центр исследования технологий искусственного интеллекта

AI Technology Research

Обнаружение угроз с помощью ИИ/ усиление ИБ-решений алгоритмами ИИ

Безопасность ИИ

Исследование генеративного ИИ

Центр сервисов по кибербезопасности

Security Services

Управляемая защита

Реагирование на инциденты

Оценка компрометации

Консалтинговые сервисы для центров мониторинга

Анализ защищенности

Мониторинг цифровых рисков

Центр исследования безопасности промышленных систем

ICS CERT

Анализ угроз в индустриальных инфраструктурах

Исследование и оценка уязвимостей нулевого дня в АСУ ТП

Разработка методик, стандартов и регламентов в области промышленной кибербезопасности

Подробнее

9

Исследование угроз

>2,100,000,000 киберугроз

обнаружила компания с момента основания

4,900,000,000
кибератак

обнаружила компания в 2024 году

500 тысяч
новых вредоносных файлов

обнаруживает компания каждый день

Наши главные открытия

	Expetr/ Notpetya	Olympic destroyer	Shadow hammer	Tajmahal	Mosaicregressor	Ghostemperor	Moonbounce	Операция Триангуляция	Grandoreiro
Обнаружение	2017	2018	2018	2019	2020	2021	2022	2023	2024
Начало активности	2017	2017	2018	2013	2017	2020	2021	2019	2016
Классификация	Кампания по уничтожению данных	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	Сложная целевая атака	Финансовые киберпреступления
Описание	Программа-вайпер для удаления данных под видом программы-вымогателя использовала модифицированные эксплойты EternalBlue и EternalRomance. Эксперты связывают ExPetr с BlackEnergy APT	Кибергруппа, которая атаковала организаторов, поставщиков и партнёров Зимних Олимпийских игр в Пхеньяне разрушительным сетевым червём	В результате сложной атаки на систему обновления ПО популярного производителя компьютеров вредоносная программа, замаскированная под обновление ПО, была распространена примерно на 1 миллион компьютеров с ОС Windows и подписана с помощью легитимного сертификата	Технически сложный APT-фреймворк для кибершпионажа. В него входит около 80 вредоносных модулей и функциональность, ранее не замеченная в сложных кибератаках, например возможность красть информацию из файлов, стоящих в очереди на печать, и записывать информацию, обнаруженную при первом подключении USB-носителя к ПК, при следующем подключении	Сложный модульный шпионский фреймворк, который использует буткит UEFI , основанный на исходниках утекшего в сеть буткита группы Hacking Team	Скрытное, сложное многоступенчатое вредоносное ПО, включающее руткит режима ядра Windows. Развертывается через ProxyLogon через несколько дней после раскрытия уязвимости	Сложный руткит для прошивки UEFI , который эксперты приписывают кибергруппе APT41. Он позволяет атакующим закрепляться в системе через вредоносный драйвер.	Заражение происходило через эксплойты с нулевым кликом через платформу iMessage. Вредоносная программа запускается с привилегиями root, получая полный контроль над устройством и данными пользователя	Сложный бразильский банковский троянец из семейства Tetrade позволяет атакующим обходить механизмы банковской безопасности и совершать мошеннические операции. Несмотря на аресты в 2021 и 2024 гг. , Grandoreiro остаётся наиболее активной глобальной киберугрозой. Новая, облегчённая версия троянца нацелена на 30 банков в Мексике. На атаки Grandoreiro пришлось около 5% от всех атак банковских троянцев, Всего в 2024 году разные версии зловреда были нацелены на пользователей более 1700 финансовых институтов
Цели	По всему миру, но преимущественно украинские, российские и западноевропейские компании. Более половины атакованных компаний относятся к промышленному сектору	Организации, имеющие отношение к Зимним Олимпийским играм 2018 года; 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 целей 600 систем, определенных по специальным MAC-адресам	Дипломатические представительства , чья деятельность связана с КНДР	Правительственные организации и телекоммуникационные компании	Холдинговые компании и поставщики промышленного оборудования	Устройства на iOS	Финансовые учреждения в более чем 40 странах в Северной и Латинской Америках и Европе

Целевые атаки: хронология ключевых исследований

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

2022

- Tomiris
- ZexCone
- SilentMarten
- MoonBounce
- ToddyCat
- MagicKarakurt
- CosmicStrand
- SBZ
- StripedFly
- DiceyF
- MurenShark

2023

- PowerMagic
- CommonMagic
- Trila
- LoneZerda
- CloudWizard
- Operation Triangulation
- BlindEagle
- Mysterious Elephant
- BadRory
- Dark Caracal
- HrServ

2024

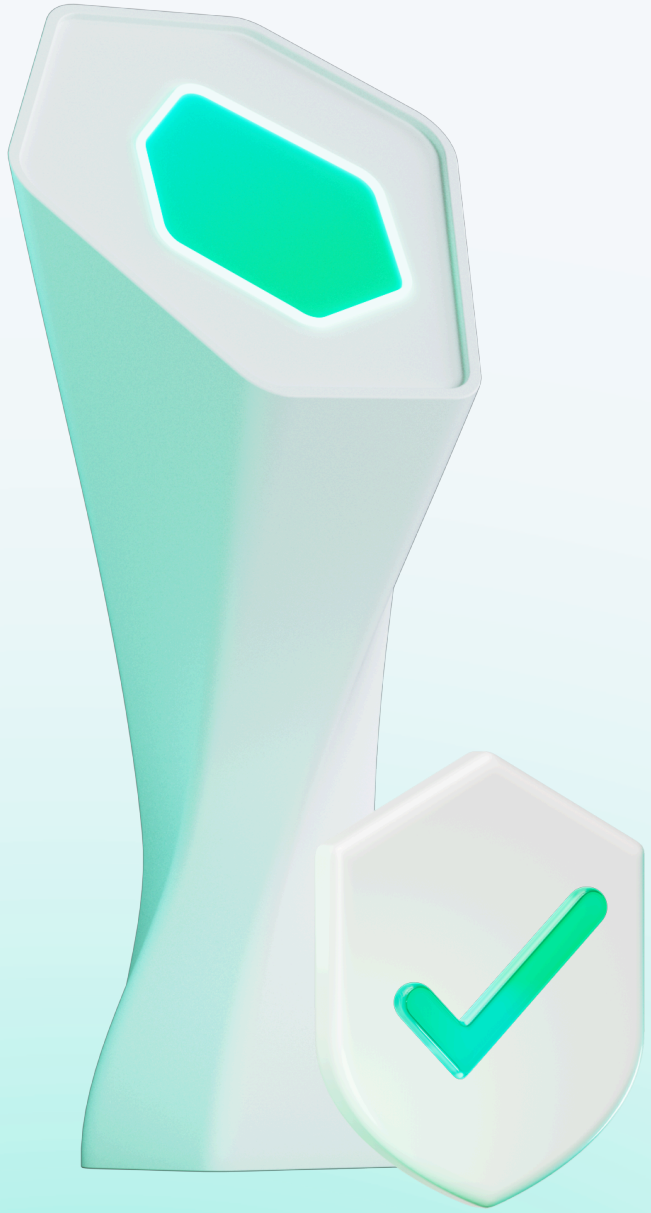
- CloudSourcerer
- PipeMagic
- Zanubis
- SambaSpy
- SideWinder
- BellaCPP
- EastWind
- PassiveNeuron
- Awaken Likho

12

Больше тестов
Больше наград*
Больше защиты

Поскольку кибербезопасность становится жизненно важной для каждой организации и каждого человека, доверие к поставщикам имеет огромное значение. Мы защищаем корпоративных клиентов и частных пользователей по всему миру, и признание международных независимых агентств очень важно для нас. В 2024 году наши продукты принимали участие в 95 независимых тестах и обзорах, 92 раза вошли в тройку лучших и 91 раз заняли первое место.

kaspersky.ru/top3



95

тестов / обзоров

91

раз заняли первое место

в **97%**

случаев наши решения попадали в топ-3

«Лаборатория Касперского» и ИИ

Компания активно участвует в российских и международных альянсах, разрабатывая этические стандарты в области ИИ и предоставляя экспертный взгляд в регуляторных обсуждениях

Альянс в сфере ИИ

«Лаборатория Касперского» — член Альянса в сфере ИИ. Он объединяет ведущие технологические компании с целью ответственного развития на основе искусственного интеллекта в России

AIM Global

«Лаборатория Касперского» — член Глобального альянса по искусственному интеллекту для промышленности и производства, созданного в 2023 году ООН по промышленному развитию (UNIDO)

Пакт Европейской комиссии об ИИ

«Лаборатория Касперского» подписала Пакт об ИИ.

Это инициатива Европейской комиссии, направленная на создание общей нормативно-правовой базы для использования искусственного интеллекта

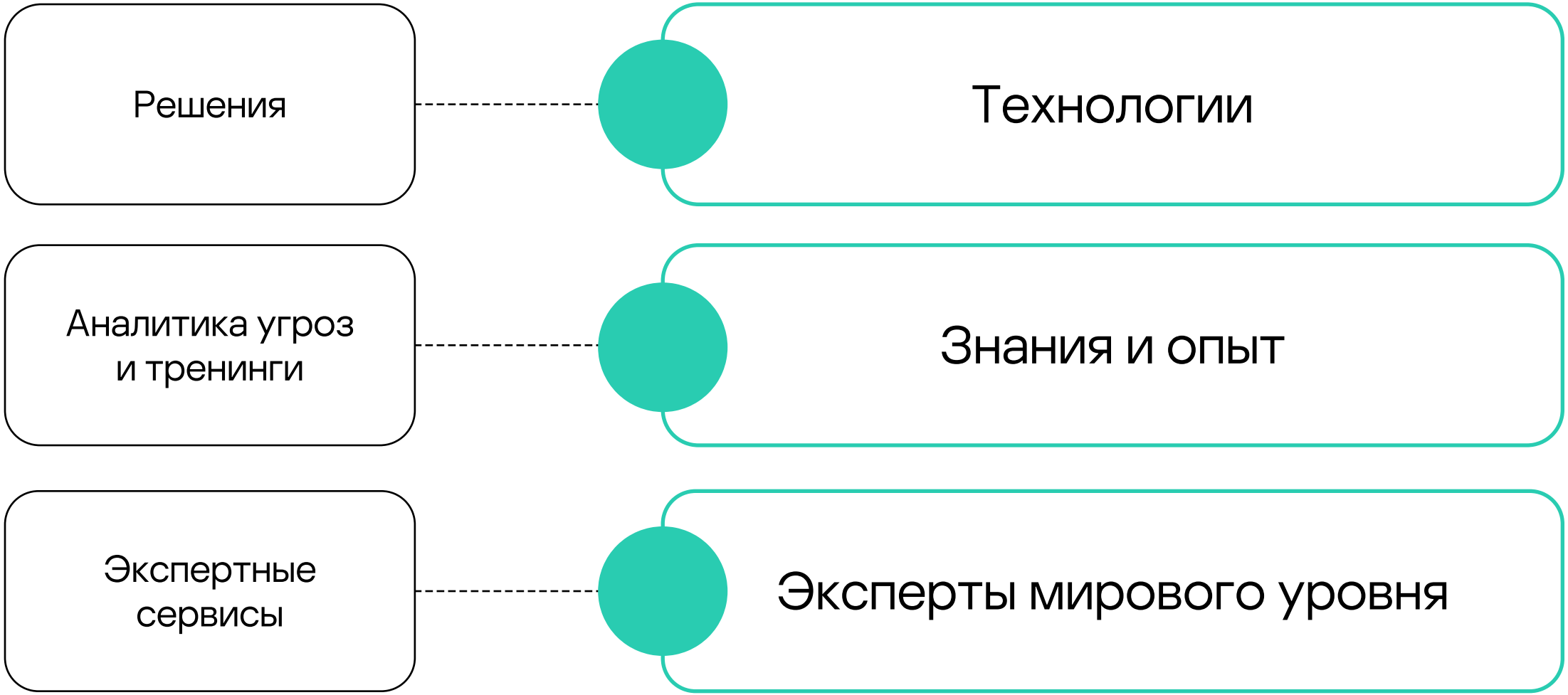
Принципы этичного использования ИИ в кибербезопасности

На Форуме по управлению Интернетом в 2023 году «Лаборатория Касперского» представила принципы, описывающие этичное применение ИИ в сфере кибербезопасности

Руководство по безопасной разработке ИИ

На Форуме по управлению интернетом в 2024 году «Лаборатория Касперского» представила Руководство по безопасной разработке и внедрению систем на основе ИИ, призванное помочь разработчикам и специалистам по кибербезопасности избежать киберрисков, связанных с ИИ

Экспертиза в основе портфолио «Лаборатории Касперского»



Безопасная, гибкая и масштабируемая операционная система для построения надёжной основы для ИТ-среды

Микроядерная архитектура

Обеспечивает прозрачность и строгий контроль качества кода, отказоустойчивость и масштабируемость ОС

Изоляция компонентов

Все компоненты полностью изолированы друг от друга и от внешней среды, что исключает неконтролируемые взаимодействия



Управление межпроцессным взаимодействием

Любое взаимодействие между компонентами, которое явно не разрешено политикой безопасности, автоматически запрещается

Кибериммунитет

Созданные в соответствии со специальной методологией и процессами, продукты и решения на KasperskyOS обладают встроенной устойчивостью даже к совершенно новым киберугрозам

Сферы применения

Инфраструктура тонкого клиента

Операционная система для тонких клиентов основана на микроядре KasperskyOS

Транспорт

ПО для высокопроизводительных контроллеров в автомобилях, которое сочетает функции телематического контроля и безопасного шлюза

Корпоративные мобильные устройства

ОС для корпоративных мобильных устройств основана на микроядре KasperskyOS

* Доступно только в рамках программы Early Access Program для текущих заказчиков и партнеров

16

Портфолио продуктов на KasperskyOS

Kaspersky Thin Client

Кибериммунная и функциональная инфраструктура тонких клиентов

- Kaspersky Security Center
  - Kaspersky Security Management Suite
- Kaspersky USB Redirector

Kaspersky Appicenter

Платформа для распространения цифрового контента, которая объединяет пользователей, независимых разработчиков приложений и глобальных производителей устройств на базе KasperskyOS

Kaspersky Automotive Secure Gateway

Построение надёжных IT-систем для умного автотранспорта

- Kaspersky Automotive Adaptive Platform
- Kaspersky Automotive Secure Broker Framework
- Kaspersky OTA Agent
- Kaspersky Vehicle SOC Agent
- Kaspersky Remote Diagnostic Agent

KasperskyOS Mobile

Безопасная ОС для корпоративных мобильных устройств

- Kaspersky Security Center
  - KasperskyOS Mobile Device Management

Решения «Лаборатории Касперского» для ИТ-сред

17

Защита IT-инфраструктуры

1

Фундаментальная защита | Расширенная защита | Комплексная защита и оптимизация процессов обеспечения ИБ

- Конечные точки
- Сеть
- Облачные рабочие нагрузки

Корпоративный **XDR**

Централизованный мониторинг и корреляция событий ИБ

Kaspersky Unified Monitoring and Analysis Platform

Фокусные решения

- Kaspersky Container Security
- Kaspersky SD-WAN
- Kaspersky Fraud Prevention
- Kaspersky Scan Engine
- Kaspersky Secure Mobility Management
- Kaspersky DDoS Protection

2

- Осведомленность: Kaspersky Security Awareness
- Аналитика угроз: Kaspersky Threat Intelligence
- Тренинги: Kaspersky Cybersecurity Training

3

- Анализ защищенности: Kaspersky Security Assessment
- Управляемая защита: Kaspersky Managed Detection and Response
- Реагирование на инциденты: Kaspersky Incident Response
- Оценка компрометации: Kaspersky Compromise Assessment
- SOC-консалтинг: Kaspersky SOC Consulting
- Профессиональные сервисы: Kaspersky Professional Services

18

Решения «Лаборатории Касперского» для OT-сред

Open
Single Management
Platform

1. Инструменты
2. Знания
3. Поддержка

Комплексная защита и оптимизация процессов обеспечения ИБ

1

Промышленный
XDR

Kaspersky
Industrial
Cybersecurity

Продвинутое управление активами
Расширенное обнаружение и реагирование на угрозы
Аудит безопасности

Фокусные решения

Kaspersky Antidrone
Kaspersky Machine Learning for Anomaly Detection
Kaspersky SD-WAN
Kaspersky Thin Client
Kaspersky Automotive Secure Gateway

Расширенная защита

Kaspersky Industrial CyberSecurity for Nodes — Конечные устройства, SCADA

Kaspersky Industrial CyberSecurity for Networks — Сетевое оборудование, контроллеры и IIoT-устройства

2

Осведомленность	Аналитика угроз	Тренинги
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

3

Анализ защищенности	Управляемая защита	Реагирование на инциденты	Профессиональные сервисы
Kaspersky ICS Security Assessment	Kaspersky Managed Detection and Response	Kaspersky Incident Response	Kaspersky Professional Services

19

Kaspersky Threat Intelligence

Машиночитаемые аналитические данные об угрозах

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Поддержка экспертов по борьбе с угрозами

- Kaspersky Takedown
- Kaspersky Ask the Analyst

Kaspersky Threat Intelligence

- Тактический уровень
- Операционный уровень
- Стратегический уровень

Человекочитаемые аналитические данные об угрозах

- Kaspersky Threat Lookup
- Kaspersky Threat Infrastructure Tracking
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - Crimeware
  - ICS
- Kaspersky Digital Footprint Intelligence

20

XDR-платформа для защиты корпоративной инфраструктуры

Централизованное управление всей ИБ-системой помогает ИБ-службам отражать кибератаки на всех уровнях значительно быстрее и с меньшими усилиями благодаря оптимально настроенной автоматизации защитных действий, кросс-продуктовому взаимодействию и многоуровневому контролю потенциальных точек входа злоумышленников

Kaspersky Symphony XDR

Как помогает

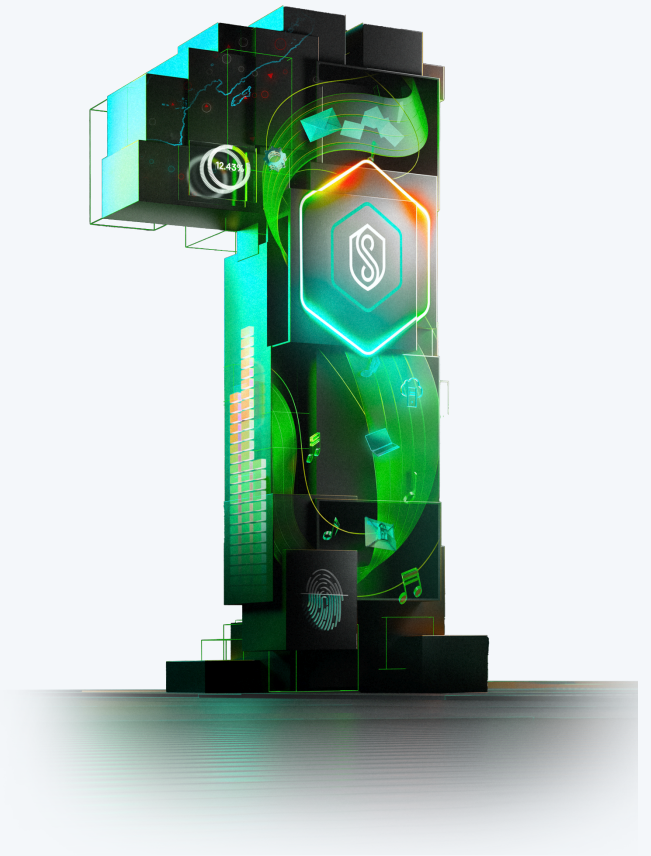
Упрощает управление инфраструктурой ИБ и помогает соответствовать требованиям регуляторов

Сокращает среднее время обнаружения сложных угроз (MTTD), а также среднее время реагирования на инциденты (MTTR)

регуляторов

Позволяет максимально автоматизировать и упростить процесс реагирования на инциденты

Оптимизирует ИБ-ресурсы и повышает операционную эффективность ИБ-команд



21

Всесторонняя защита цифровой жизни

С нашим разнообразным портфолио защитных продуктов мы вдохновляем пользователей получать все преимущества от новых технологий — они знают, что мы позаботились об их безопасности и безопасности их семей

Kaspersky Standard
Win | Android | Mac | iOS | Linux

Kaspersky Plus
Win | Android | Mac | iOS | Linux

Kaspersky Premium
Win | Android | Mac | iOS | Linux

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

PetKa
Android

Kaspersky Who Calls*
Android | iOS

Kaspersky eSIM Store
Android | iOS | Web

Решения для интернет-провайдеров

Kaspersky Safe Web
Защита на уровне сети

Kaspersky Smart Home
Предназначено для установки на домашний роутер

ИИ в «Лаборатории Касперского»: история использования



2008

Автоаналитик, который сравнивает поступающие файлы по статическим признакам с коллекцией уже известного вредоносного ПО

2010

Аналитик, использующий логи эмуляции как дополнительный критерий для кластеризации исполняемых файлов

2011

Система поиска похожих файлов на основе паттернов поведения в логах эмулированного исполнения программ у пользователей, с отправкой новых паттернов в облачные сервисы компании и их анализом при помощи ML

2013

TrueForest: создание «умных» детектирующих правил при помощи алгоритма решающих деревьев и применение их для анализа файлов в контуре компании

2014

Умное хеширование: алгоритм, создающий правила детектирования вредоносных семейств, основанный на локально-чувствительных хешах

2015

Модуль внутреннего автоаналитика, использующий для кластеризации образцов журналы их исполнения в «песочнице»

2016–2017

Алгоритмы решающих деревьев для поиска вредоносных программ доставляются и применяются на устройствах пользователей

2018

- ИИ-автоаналитик для Kaspersky MDR
- Применение ИИ становится всё более распространённым в продуктах, с которыми конечный пользователь взаимодействует напрямую — для анализа поведения исполняемых файлов
- Адаптивный контроль аномалий: выделяется типичное поведение системы, и детектируются отклонения от него
- MLAD. система раннего обнаружения аномалий в промышленных данных

2020

- Система карантина для спам-писем на основе глубоких нейронных сетей

2022

- Новая система обнаружения фишинга на основе машинного обучения

2023

- Система анализа графа веб-страниц для поиска вредоносной активности
- Пользовательские ML-модели в MLAD

2024

- Сервис безопасности на базе ИИ https://ai-cert.kaspersky.ru/
- ИИ для KUMA/XDR (расчет степени риска для хостов)
- Генеративный ИИ для обобщения аналитики угроз
- ИИ-ассистент для помощи в анализе киберугроз (Kaspersky Investigation and Response Assistant, KIRA)

2025

- Появление в KUMA ИИ-функциональности для обнаружения атак с подменой DLL
- Детектирование украденных аккаунтов в MDR и KUMA/XDR
- Новые навыки ассистента KIRA в продуктах KUMA, XDR, EDR и KCS
- Интеграция ИИ-агентов в VM

Прозрачность и унификация процессов



2 дата-центра

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

Здесь мы обрабатываем и храним данные пользователей из Европы, Северной и Латинской Америк, Ближнего Востока и нескольких стран Азиатско-Тихоокеанского региона.



13 Центров прозрачности

В Бразилии, Колумбии, Италии, Японии, Малайзии, Нидерландах, Руанде, Саудовской Аравии, Сингапуре, Южной Корее, Испании, Швейцарии и Турции



2 регулярных независимых оценки

Они подтверждают доверенность практик разработки, принятых в «Лаборатории Касперского»:

- Аудит SOC 2
- Сертификация ISO 27001



$8,4 млн

С 2018 года «Лаборатория Касперского» инвестировала более $8.4 млн в свою Глобальную инициативу по информационной открытости, в том числе $5.6 млн на оборудование для дата-центров в Цюрихе



66 брифингов в Центрах прозрачности

для представителей государственных органов и частных компаний



70 отчётов об уязвимостях в рамках программы Bug Bounty

Общая сумма выплат независимым исследователям составила 92,930 долларов США

ESG

ESG-отчет компании хранится здесь:
https://esg.kaspersky.com/ru/

1

Этика и прозрачность

- Прозрачность исходного кода и процессов
- Защита данных и права на приватность
- Управление прозрачностью и устойчивостью бизнеса

2

Киберустойчивость

- Защита критической инфраструктуры
- Помощь в расследовании киберпреступлений на глобальном уровне
- Защита пользователей от киберугроз

3

Забота об окружающей среде

- Сокращение воздействия на окружающую среду от работы наших инфраструктур, операций и продуктов

4

Возможности для людей

- Забота о сотрудниках
- Инклюзивность и доступность технологий
- Развитие талантов в ИТ

5

Технологии будущего

- Кибериммунитет для новых технологий

Обучаем кибербезопасности

Школа

«Лаборатория Касперского» просвещает школьников всех возрастов – от младших до старших классов

- Азбука кибербезопасности
- Урок Цифры
- Enter IT

Университет

В рамках международного образовательного проекта Kaspersky Academy мы сотрудничаем с вузами по всему миру и предлагаем студентам возможности для начала карьеры

- Kaspersky Academy Alliance
- SafeBoard
- Курс «ИТ-журналистика»

ИБ-специалисты

«Лаборатория Касперского» запустила в России платформу с онлайн-тренингами для ИТ- и ИБ-специалистов

- Экспертные тренинги
- Карта профессий в ИБ

Повышение уровня цифровой грамотности

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.

Бесплатный онлайн-курс «Кибергигиена»

Бесплатный онлайн-курс о безопасности в интернете рассчитан на широкую аудиторию и охватывает основные вопросы цифровой безопасности

Подробнее

Уведомление о слежке

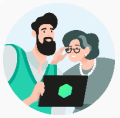
В приложении Kaspersky есть функция уведомления пользователя о подброшенных Bluetooth-устройствах, в том числе беспроводных метках, и функция защиты от сбора данных о пользователе

Подробнее

Проверка настроек

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

Подробнее



Сериал о кибермошенничестве

Документальный сериал «Эволюция обмана» — совместный просветительский проект с М.Видео Эльдорадо

Подробнее

Спонсорства и партнерства



Спорт

Kaspersky Race — это ежегодный спортивный фестиваль, который проводится с 2020 года. Вклад компании в спортивное комьюнити Беларуси. На нём представлены дистанции разного уровня сложности для бегунов и велосипедистов, детей и взрослых



Искусство

«Лаборатория Касперского» — партнер по кибербезопасности Большого театра



Киберспорт

«Лаборатория Касперского» — партнер нескольких киберспортивных команд из разных стран

Активируй будущее



kaspersky