О «Лаборатории Касперского»

kaspersky

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
«Лаборатории Касперского»

О компании

Компания основана в 1997 году, возглавляется Евгением Касперским. Разрабатывает инновационные ИТ-решения для защиты корпоративных и домашних пользователей

200 стран и территорий

30+ офисов по всему миру

> 5000 специалистов

>1 млрд

устройств защищено от массовых киберугроз и целенаправленных атак*

>200 тыс.

корпоративных клиентов по всему миру

Центры прозрачности **Офисы**

* Цифра основана на данных Kaspersky Security Network (KSN) по автоматизированному анализу вредоносных программ и включает записи с 2011 года

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 уникальных центров экспертизы

467 тыс. новых вредоносных файлов обнаруживает компания ежедневно

>2 млрд киберугроз обнаружила компания с момента своего основания

Центры экспертизы

Глобальный центр исследования и анализа угроз

GREAT

- Исследование наиболее сложных атак: кампаний кибершпионажа, глобальных киберэпидемий
- Анализ сложного финансового вредоносного ПО
- Безопасность инновационных технологий

Исследование угроз

Threat Research

- Anti-Malware Research
- Content Filtering Research
- SSDLC & Secure-by-Design Methodologies

ИИ-разработки

AI Technology Research

- AI-Powered Threat Detection / Solutions
- AI Cybersecurity
- GenAI Research

Услуги кибербезопасности

Security Services

- MDR
- Реагирование на инциденты
- Оценка уровня защищенности
- SOC Consulting
- Digital Footprint Intelligence

Kaspersky ICS CERT

ICS CERT

- Critical Infrastructure Threat Analysis
- Technology Associations, Analytics and Standards
- ICS Vulnerability Research and Assessment

Исследование угроз

Анализ инцидентов

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

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

Награды

Больше тестов.
Больше наград*
Больше защиты

*Kaspersky.com/top3

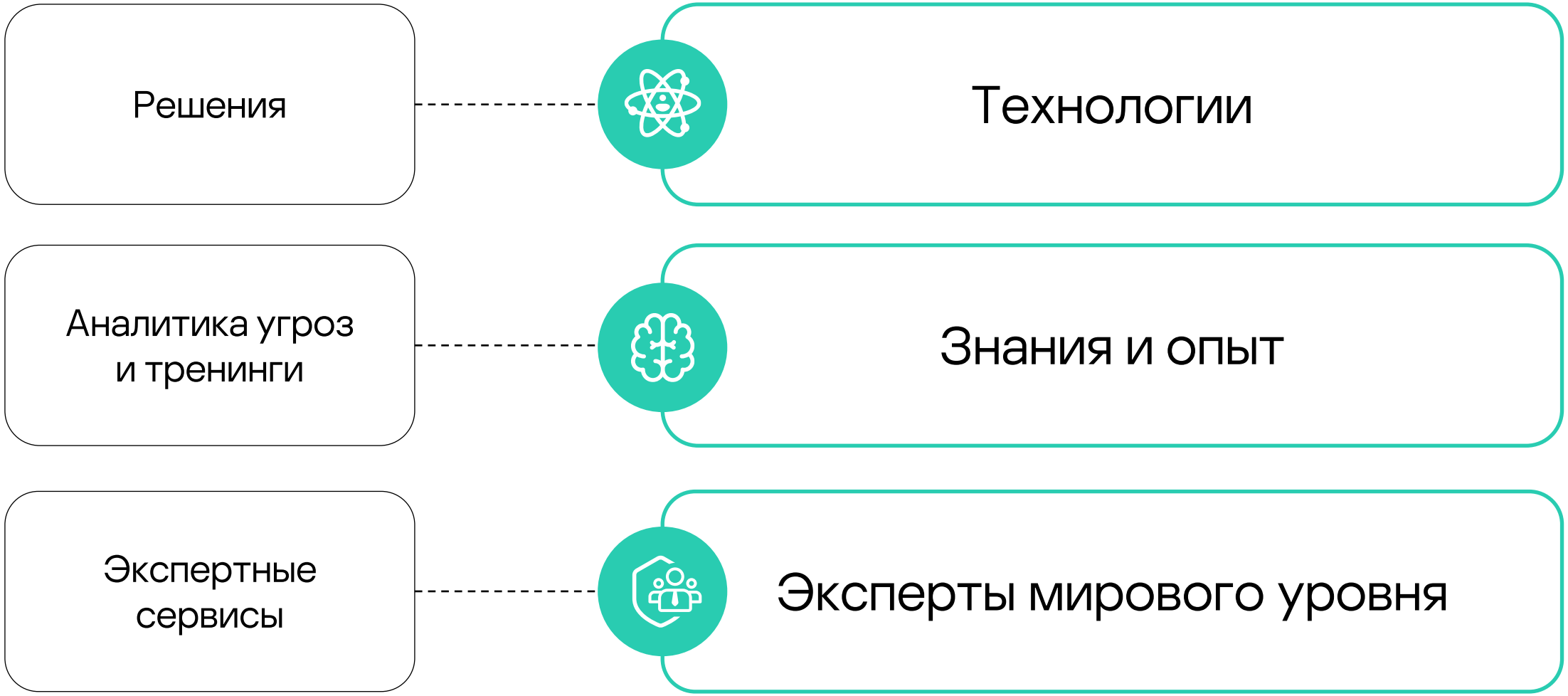
95
тестов/
обзоров

91
раз заняли
первое место

В **97%**
случаев наши
решения
попадали в топ-3

Поскольку кибербезопасность становится жизненно важной для каждой организации и каждого человека, доверие к поставщикам имеет огромное значение. Мы защищаем корпоративных клиентов и домашних 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.

Экспертиза в основе портфолио «Лаборатории Касперского»



Подход и методология «Лаборатории Касперского» в области разработки исходно безопасных (Secure-by-Design) ИТ-систем

Подавляющее число атак на кибериммунные системы не могут повлиять на выполнение ими критических функций

Архитектурный подход создает среду, в которой уязвимости или ошибки в коде не представляют угрозы

Методология, технологии и инструменты для создания кибериммунных решений

KasperskyOS — оптимальная платформа для построения кибериммунных ИТ-систем

Микроядерная операционная система компании для ИТ-продуктов с высокими требованиями к кибербезопасности

Предоставляет платформу для создания исходно безопасных (Secure-by-design) решений

Создает среду, которая не позволяет приложениям выполнять незадекларированные функции и предотвращает эксплуатацию уязвимостей

Дает полную прозрачность, гибкую конфигурацию политик кибербезопасности и контроль над взаимодействием по всей системе

Сферы применения

- Интернет вещей и промышленный интернет вещей
- Транспорт
- Корпоративные мобильные устройства
- Контроллеры для умных городов
- Инфраструктура тонкого клиента

Что мы предлагаем

Решения «Лаборатории Касперского»

Растущая сложность угроз

3 Сложные кибератаки

2 Передовые угрозы

1 Массовые угрозы

Ресурсы

Kaspersky Expert Security
Команда ИБ или SOC

Kaspersky Optimum Security
ИБ-специалист

Kaspersky Security Foundations
IT-специалист

Требуемый инструментарий для отражения

Мощный EDR	SIEM	NTA с сетевой песочницей	Для изолированных сред
Kaspersky Endpoint Detection and Response	Kaspersky Unified Monitoring and Analysis Platform	Kaspersky Anti Targeted Attack	Kaspersky Private Security Network

Базовый EDR	Хостовая песочница	Платформа киберграмотности
Kaspersky EDR для бизнеса Оптимальный	Kaspersky Sandbox	Kaspersky Automated Security Awareness Platform

Фокусные решения

- Для территориально-распределенных сетей: Kaspersky SD-WAN
- Защита контейнеров: Kaspersky Container Security
- Защита онлайн-ресурсов от DDoS атак: Kaspersky DDoS Protection
- Защита внутренних систем от угроз из файлов: Kaspersky Scan Engine
- Защита гражданских объектов от дронов: Kaspersky Antidrone
- Решения на базе микроядерной ОС: KasperskyOS

Малый бизнес		Средний и крупный бизнес					
Kaspersky Endpoint Security Cloud	Kaspersky Small Office Security	Kaspersky Security для бизнеса	Kaspersky Security для виртуальных и облачных сред	Kaspersky Secure Mobility Management	Kaspersky Embedded System Security	Kaspersky Security для почтовых серверов	Kaspersky Security для интернет-шлюзов
Защита конечных устройств						Защита сети и почты	

Сервисы «Лаборатории Касперского»

Растущая сложность угроз

3 Сложные кибератаки

2 Передовые угрозы

1 Массовые угрозы

Ресурсы

Kaspersky Expert Security

Команда ИБ или SOC

Kaspersky Optimum Security

ИБ-специалист

Kaspersky Security Foundations

IT-специалист

Рекомендации по экспертным сервисам

Повышение экспертизы	Аналитика угроз	Анализ компрометации	Управляемая защита	Реагирование на угрозы	Анализ защищенности
Kaspersky Cybersecurity Training	Kaspersky Threat Intelligence	Kaspersky Compromise Assessment	Kaspersky MDR	Kaspersky Incident Response	Kaspersky Security Assessment

Системный подход к тренингам в сфере IT-безопасности

Обогащение данными	Оценка навыков сотрудников	Онлайн курс для IT-специалистов	Интерактивная командная игра	Управляемая защита
Kaspersky Threat Intelligence Portal (OpenTIP)	Kaspersky Gamified Assessment Tool	Kaspersky Cybersecurity for IT Online	Kaspersky Interactive Protection Simulation	Kaspersky MDR

Поддержка

- Сервисы расширенной технической поддержки (MSA)
- Kaspersky Professional Services

Формирование ИБ-процессов и построение SOC

- **Kaspersky SOC Consulting**
- **Kaspersky Tabletop Exercise**
- **Kaspersky Adversary Attack Emulation**

Защита корпоративного сегмента

Защита промышленных инфраструктур

Kaspersky Symphony

Всеобъемлющая киберзащита бизнеса
в виртуозном исполнении

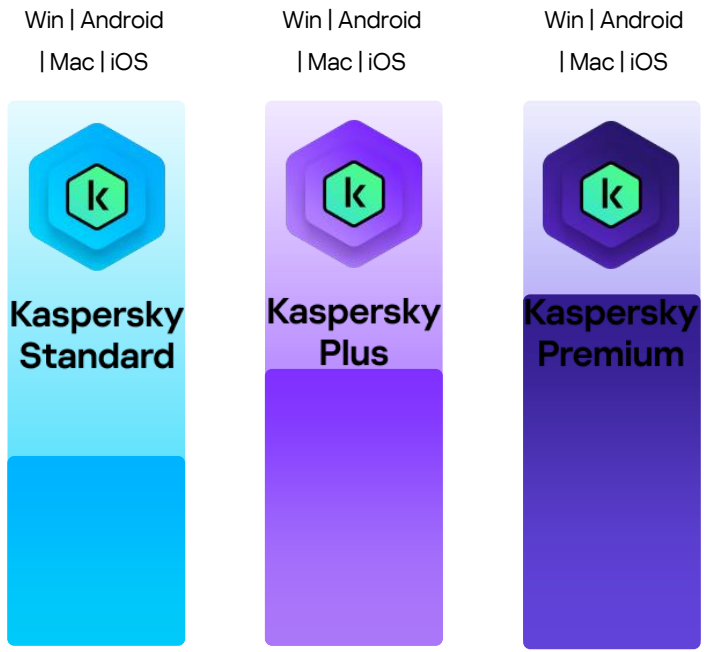
Kaspersky OT CyberSecurity

Сплав технологий и экспертизы
для промышленной кибербезопасности

Портфолио решений для домашних пользователей

Мы вдохновляем наших пользователей получать все преимущества от новых технологий. Наши клиенты знают, что мы позаботились об их безопасности

- Премиум-сервисы
- Умный дом
- Защита от кражи личности
- Приватность
- Производительность
- Безопасность



Kaspersky Who Calls
Android | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Развитие индустрии

Мы развиваем индустрию через:

Устойчивое развитие

Мы строим безопасное будущее и заинтересованы не только в цифровой сохранности мира. Снижение негативного воздействия на окружающую среду, забота о сотрудниках, доступность технологий — ключевые направления для компании.

Образовательные инициативы

Создаем образовательные проекты на основе собственного опыта и исследований, направленные на повышение уровня осведомленности в цифровой сфере, а также делимся знаниями об информационной безопасности для противодействия киберугрозам.

Взгляд в будущее

Спонсорские и партнерские проекты компании отражают подход «Лаборатории Касперского», ориентированный на будущее, профессионализм и честность во всем, что мы делаем.

Поддерживаемые проекты подтверждают достижения в науке, культуре, спорте и технологиях.

Прозрачность и унификация процессов

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.

13 Центров прозрачности

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

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.

2 регулярных независимых оценки

SOC 2

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 Type 2 в 2023 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.

Proven.
Transparent.
Independent.

ESG

Наша миссия — строить безопасное будущее, чтобы технологии улучшали не только повседневную жизнь людей, но и жизнь на планете в целом. Мы выполняем эту миссию, повышая устойчивость цифрового пространства к угрозам, уделяя при этом особое внимание социальным проектам и инициативам для повышения осведомленности об экологической повестке.

Пять подходов к ведению бизнеса

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 нашей 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

Узнайте больше в ESG-отчете компании с результатами за вторую половину 2022 и весь 2023 год

Повышение знаний о кибербезопасности

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

Подробнее

Защита от сталкерского ПО

Решения компании для домашних пользователей предлагают лучшую в своем классе защиту и умеют обнаруживать программы, используемые для тайной слежки

Подробнее

Privacy Checker

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

Подробнее

Kids Safe Media

Медиа о детской онлайн-безопасности для детей и родителей

Подробнее

Спонсорства и партнерства

Как глобальная инновационная компания, 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, сохраняем культурное наследие и даем спортсменам возможность реализовать свой потенциал по максимуму.

Искусство

«Лаборатория Касперского» — партнер по кибербезопасности Большого театра

Мотоспорт

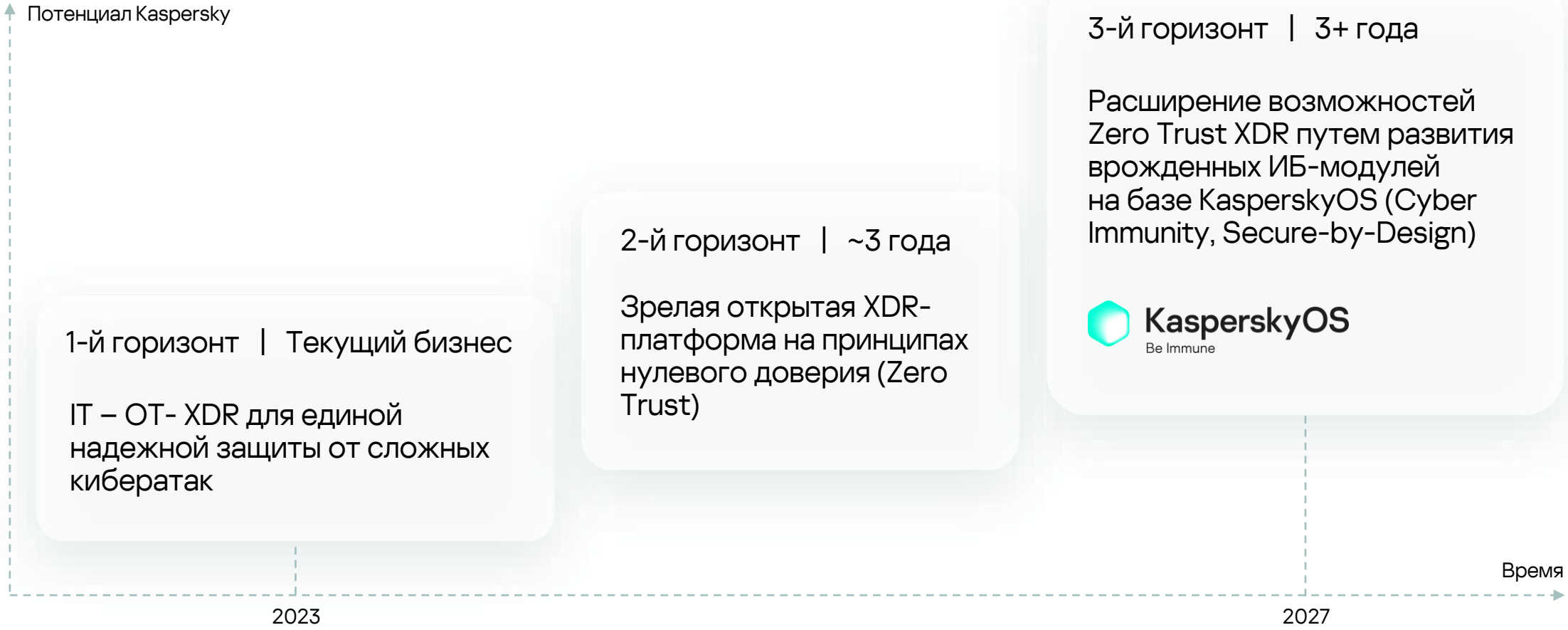
«Лаборатория Касперского» поддерживает талантливых пилотов, таких как Амна и Хамда Аль Кубаиси, первых эмиратских гонщиц

Киберспорт

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

Учет перспектив ИБ в настоящем

Горизонты продуктового развития Kaspersky в 2023-2027 гг.



Активируй будущее

Россия, Москва, 125212
Ленинградское шоссе, д.39А, стр.3
БЦ «Олимпия Парк»

+7-495-797-8700; +7-495-795-0275
info@kaspersky.com
www.kaspersky.com