

# О «Лаборатории Касперского»

kaspersky



Евгений Касперский  
Генеральный директор  
«Лаборатории Касперского»

“

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.

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

**>220 тыс.**

корпоративных клиентов  
по всему миру

Центры прозрачности

Офисы

## 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

**>1,4 млрд**

киберугроз обнаружила  
«Лаборатория Касперского»  
с момента своего основания

**>411 тыс.**

новых вредоносных файлов  
обнаруживает «Лаборатория  
Касперского» ежедневно

**>200**

крупных кибергрупп  
отслеживается нами



# Центры экспертизы по исследованиям угроз и расследованиям инцидентов

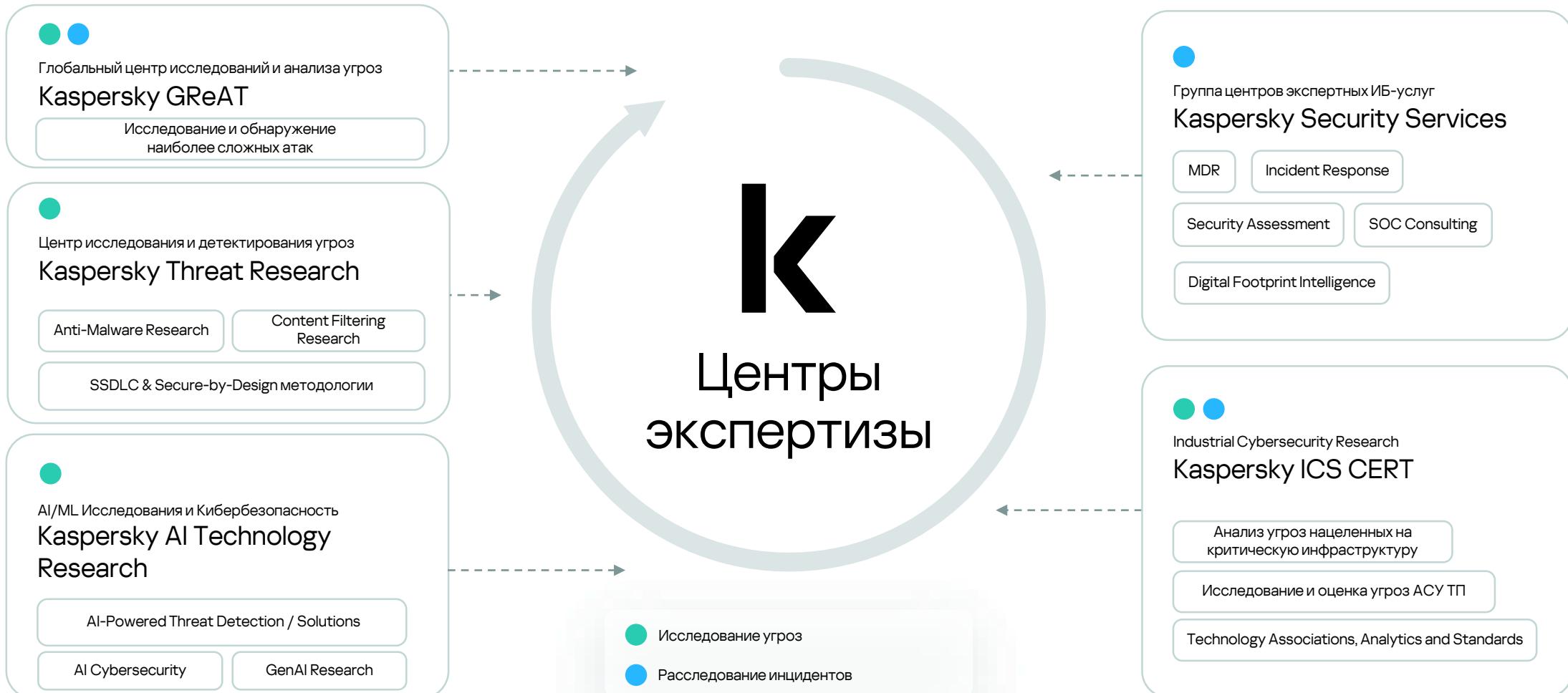
5

Пять глобальных центров используют опыт и знания «Лаборатории Касперского» для выявления, исследования угроз и противодействия им

	GReAT	Threat Research	Kaspersky ICS CERT	Security Services	Kaspersky AI Technology
Центр	Глобальный центр исследований и анализа угроз	Центр исследования и детектирования угроз	Центр исследования безопасности промышленных систем	Группа центров экспертных ИБ-услуг	AI/ML Исследования и Кибербезопасность
Задачи	<ul style="list-style-type: none"><li>Поиск и исследование наиболее сложных атак, кампаний кибершпионажа, новых методов заражения, экспloitов, использующих уязвимости нулевого дня</li><li>Аналитика APT-угроз</li><li>Основа для APT Intelligence Reporting и Crimeware Intelligence Reporting</li></ul>	<ul style="list-style-type: none"><li>Два направления: Anti-Malware Research (AMR) и Content Filtering Research (CFR)</li><li>Обеспечение защиты от киберугроз (вредоносное ПО – включая шифровальщики, спам, фишинг, и т.д.)</li><li>Разработка методологии для обнаружения киберугроз (правила детектирования)</li><li>Развитие новых технологий ИИ и кибербезопасности</li></ul>	<ul style="list-style-type: none"><li>Исследование угроз и уязвимостей промышленных систем</li><li>Оценка состояния кибербезопасности продуктов АСУ ТП / IoT и процессов их разработки</li><li>Разработка методики, стандартов и регламентов в области промышленной кибербезопасности</li></ul>	<ul style="list-style-type: none"><li>Управляемая защита MDR (на базе Kaspersky SOC)</li><li>Мониторинг цифровых рисков (DFI)</li><li>Реагирование на инциденты (Incident Response)</li><li>Анализ систем защищенности (Security Assessment)</li><li>Консалтинг по построению SOC (SOC Consulting)</li></ul>	<ul style="list-style-type: none"><li>Product Security team – управление безопасностью решений Kaspersky через организацию безопасной разработки (SSDLC) и bug bounty программы</li><li>KasperskyOS Development – разработка кибериммунных продуктов и методологии создания безопасного ПО согласно принципу Secure-by-Design</li></ul>

# Центры экспертизы «Лаборатории Касперского»

6



# Целевые атаки: хронология ключевых исследований

7

Глобальный центр исследований и анализа киберугроз (GReAT) известен во всем мире благодаря расследованиям самых сложных кибератак.

The timeline consists of a horizontal dashed teal arrow at the top, with years from 2016 to 2023 placed below it. Each year is enclosed in a rounded rectangular box. Below each year box is a list of specific targeted attack names, also enclosed in rounded rectangular boxes. The attacks are listed in chronological order from left to right within each year's box.

2016	2017	2018	2019	2020	2021	2022	2023
ProjectSauron	WannaCry	Zebrocy	Topinambour	Cycldek	GhostEmperor	ZexCone	Operation Triangulation
StrongPity	Shamoon 2.0	DarkTequila	ShadowHammer	SixLittleMonkeys (aka Microcin)	ExCone	SilentMarten	
Lazarus	StoneDrill	MuddyWater	SneakyPastes	CactusPete	BlackShadow	MoonBounce	CommonMagic
Fruity Armor	BlueNoroff	Skygofree	FinSpy	DeathStalker	BountyGlad	ToddyCat	
ScarCruft	ExPetr / NotPetya	Olympic Destroyer	DarkUniverse	MATA	EdwardsPheasant	MagicKarakurt	
Poseidon	Moonlight Maze	Destroyer	COMpfun	TransparentTribe	HotCousin	CosmicStrand	
Danti	ShadowPad	ZooPark	Titanium	WellMess	GoldenJackal	SBZ	
Dropping Elephant	BlackOasis	Hades		TwoSail Junk	FerociousKitten	StripedFly	
	Silence	Octopus		MontysThree	ReconHellcat	DiceyF	
	WhiteBear	AppleJeus		MosaicRegressor	CoughingDown	MurenShark	
				VHD Ransomware	MysterySnail		
				WildPressure	CraneLand		
				PhantomLance	Tomiris		

# Наши главные открытия

	<b>Sofacy</b>	<b>Duqu 2.0</b>	<b>Lazarus</b>	<b>Project Sauron</b>	<b>Expetr / Notpetya</b>	<b>Olympic destroyer</b>
Обнаружение	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2016</b>	<b>2017</b>	<b>2018</b>
Начало активности	2008	2014	2009	2011	2017	2017
Классификация	ПО для кибершпионажа	Комплексная платформа для кибератак	Кибершпионаж и саботаж, финансовые атаки	ПО для кибершпионажа	Кампания по уничтожению данных	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	Организации, имеющие отношение к Зимним Олимпийским играм 2018; европейские организации, изучающие биологические и химические угрозы; финансовые организации в России

	<b>Shadow hammer</b>	<b>Tajmahal</b>	<b>Mosaic-regressor</b>	<b>Ghostemperor</b>	<b>Moonbounce</b>	<b>CommonMagic</b>	<b>Операция Триангуляция</b>
Обнаружение	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2023</b>
Начало активности	2018	2013	2017	2020	2021	2008	2019
Классификация	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	ПО для кибершпионажа	Многомодульное шпионское ПО	ПО для кибершпионажа
Цели	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, определенных по специальным MAC-адресам	Дипломатические представительства, чья деятельность связана с Северной Кореей	Правительственные организации и телекоммуникационные компании	Холдинговые компании и поставщики промышленного оборудования	Транспортные, сельскохозяйственные, правительственные организации в Донецке, Луганске, Крыму, центральной и западной частях Украины	Сотрудники «Лаборатории Касперского»

## 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 домашних пользователей по всему миру, признание международных независимых агентств подтверждает качество решений «Лаборатории Касперского».

В 2023 году наши продукты 94 раза вошли в тройку лучших и 93 раза заняли первое место.

### Примечания

- По результатам независимых тестов корпоративных и потребительских продуктов, 2013–2023 гг.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AppEsteem, AV-Comparatives, AV-TEST, Dennis Technology Labs, ICSA Labs, Matousec, MRG Effitas, NSS Labs, PCSL, SE Labs, Testing Ground Labs, The Tolly Group, Virus Bulletin.
- Тестировались технологии защиты от известных, неизвестных и сложных угроз.

**927**

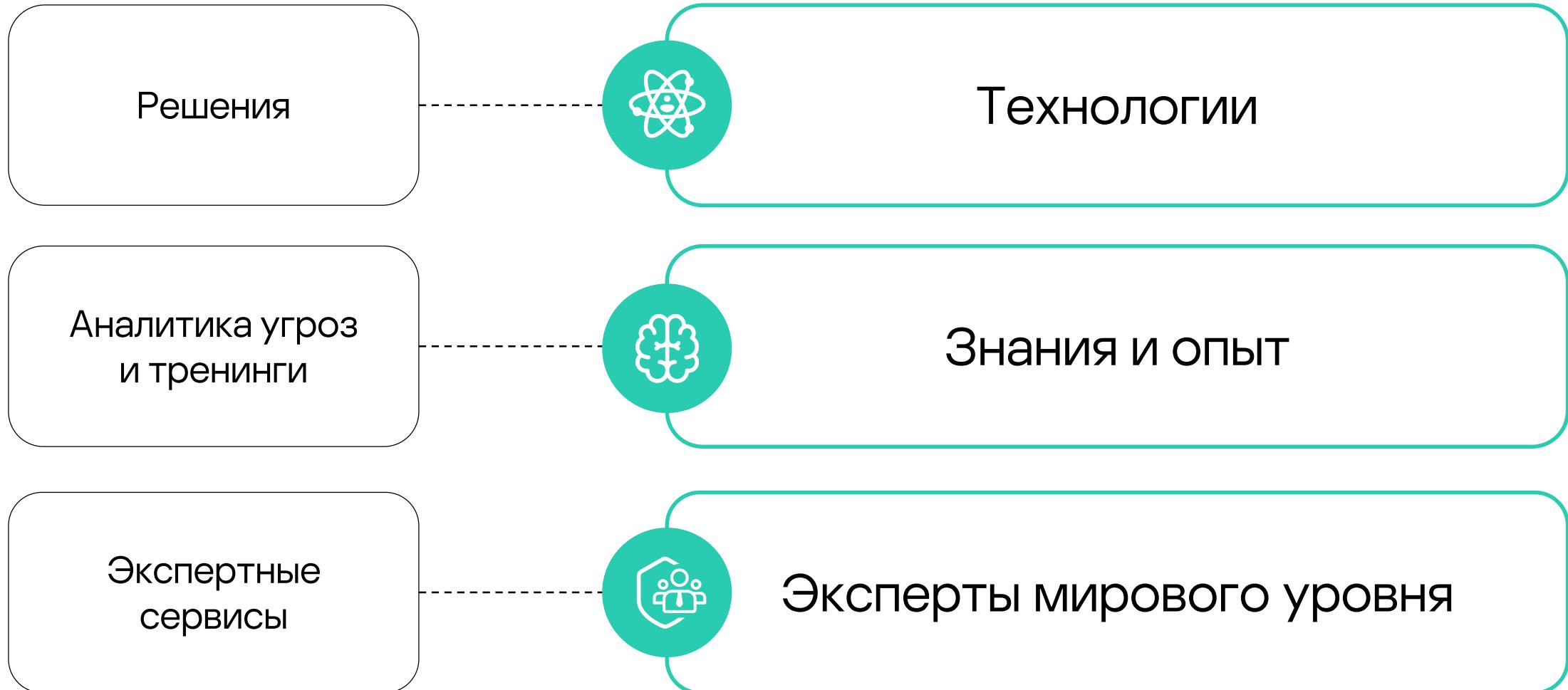
раз участвовали  
в тестах /  
обзорах  
за 2013-2023 гг.

**680**

раз заняли  
первое место

**94%**

случаев наши  
решения попадали  
в топ-3



## 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



### Сфера применения

Интернет вещей и промышленный интернет вещей

Транспорт

Корпоративные  
мобильные устройства

Контроллеры  
для умных городов

Инфраструктура  
тонкого клиента

# **Что мы предлагаем**

# Решения «Лаборатории Касперского»



# Сервисы «Лаборатории Касперского»



Экосистема защиты  
корпоративного  
сегмента



Экосистема защиты  
промышленных  
инфраструктур



Kaspersky  
Symphony

Всеобъемлющая киберзащита бизнеса  
в виртуозном исполнении



Kaspersky  
OT CyberSecurity

Сплав технологий и экспертизы  
для промышленной кибербезопасности

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

⌚️ Премиум-сервисы

🏡 Умный дом

👤 Защита от кражи личности

🔒 Приватность

📊 Производительность

🛡️ Безопасность

Win | Android  
| Mac | iOS

Win | Android  
| Mac | iOS

Win | Android  
| Mac | iOS



**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:



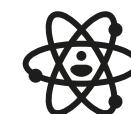
## Устойчивое развитие

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.

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 компаний.

**12** Центров  
прозрачности

В Бразилии, Италии, Японии, Малайзии, Африке, Нидерландах, Сингапуре, Испании, Швейцарии, США, Саудовской Аравии и Турции

**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.

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.

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

Подробнее

## 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 инфраструктуры, наших операций и продуктов

4

### Возможности для людей

Забота о сотрудниках  
Инклюзивность и доступность технологий  
Развитие талантов в ИТ

5

### Технологии будущего

Инновации для новых технологий  
Стремление к совершенству

# Повышение знаний о кибербезопасности

22

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](#).

## Защита от стalkerского 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](#)

## Курс по доксингу

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

[Подробнее](#)

## Kids Safe Media

Медиа о детской онлайн-безопасности для детей и родителей

[Подробнее](#)

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

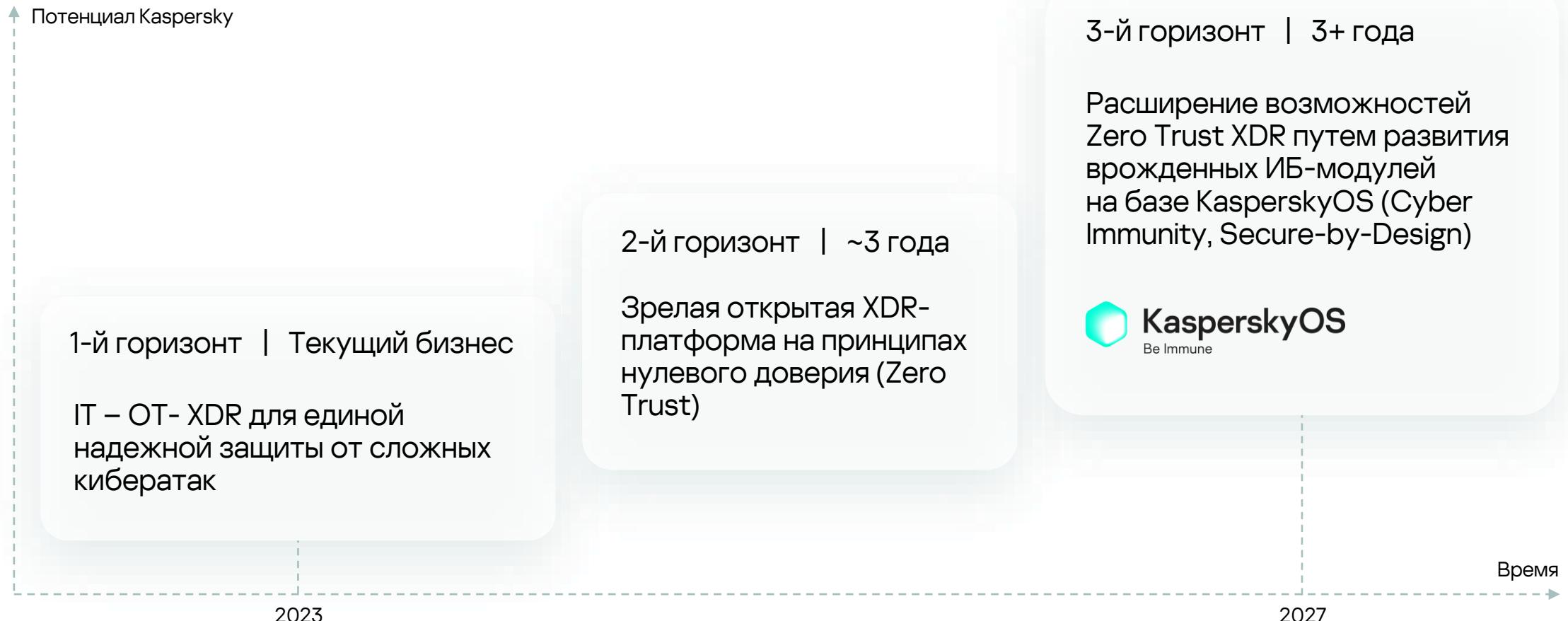
«Лаборатория Касперского» поддерживает талантливых пилотов, таких как Амна и Хамда Аль Кубаиси, первых эмиратских гонщиц



### Киберспорт

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

## 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](mailto:info@kaspersky.com)

[www.kaspersky.com](http://www.kaspersky.com)