Портфель Решений Кибербезопасности Лаборатории Касперского

Джабраил Матиев,
Директор по маркетингу в России

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

50+ Лучших мировых ИБ-экспертов, звезд в области кибербезопасности

> 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 «Лаборатории Касперского»

Все центры вносят свой вклад в
Решения Лаборатории Касперского

Центр глобальных исследований и аналитики угроз
Kaspersky GReAT

- Исследование и обнаружение наиболее сложных атак

Центр исследования и детектирования угроз
Kaspersky Threat Research

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

AI/ML Исследования и Кибербезопасность
Kaspersky AI Technology Research

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

Группа центров экспертных ИБ-услуг
Kaspersky Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Digital Footprint Intelligence

Industrial Cybersecurity Research
Kaspersky ICS CERT

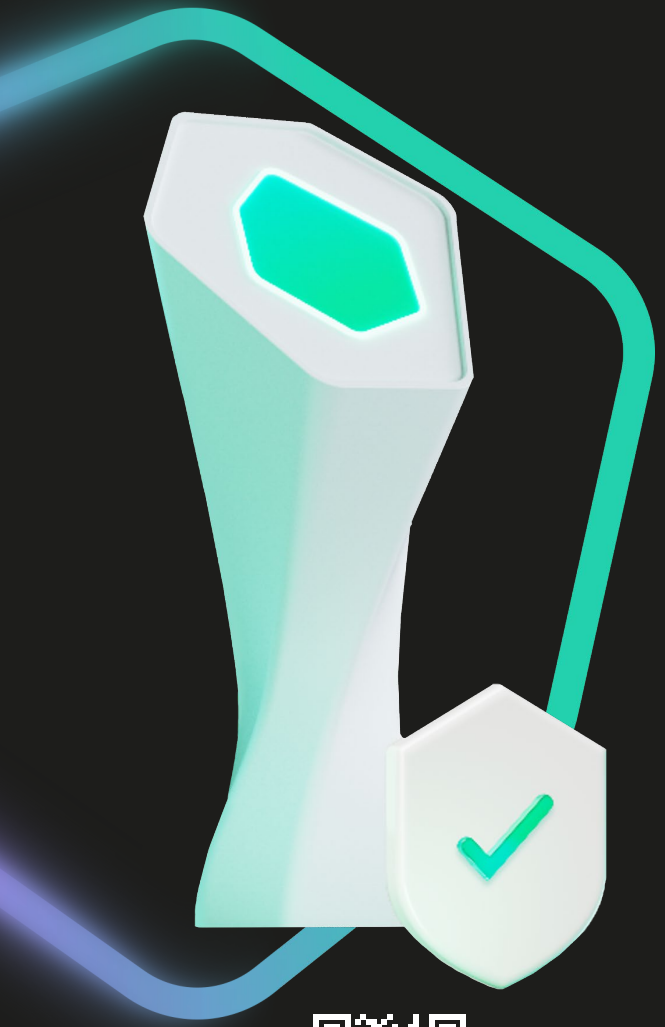
- Анализ угроз нацеленных на критическую инфраструктуру
- Исследование и оценка угроз АСУ ТП
- Technology Associations, Analytics and Standards

Исследование угроз

Расследование инцидентов

Портфолио Kaspersky

В основе — экспертиза, знания и опыт



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

в **94%**
случаев наши решения попадали в топ-3

* Kaspersky.ru/top3

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

Защита конечных устройств

Малый бизнес

- Kaspersky Endpoint Security Cloud
- Kaspersky Small Office Security

Средний и крупный бизнес

- Kaspersky Security для бизнеса
- Kaspersky Security для виртуальных и облачных сред
- Kaspersky Secure Mobility Management
- Kaspersky Embedded System Security

Защита сети и почты

- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

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**

Наш портфель услуг позволяет справиться с любой стадией кибератаки

Готовы ли вы к нападению?

Услуги для повышения вашей киберустойчивости

- Penetration testing
- Application security assessment
- Red teaming
- Incident Response Plan Assessment

Вы подозреваете, что на вас напали?

Поиск скрытых угроз, скрывающихся в вашей инфраструктуре

- Compromise Assessment (CA)
- Managed Detection and Response (MDR)

Вы подвергаетесь нападению?

Позвольте экспертам помочь вам остановить атаку - они уже помогали сотням заказчиков!

- Incident Response Retainer

Вам не хватает навыков защиты?

Давайте превратим хороших специалистов в виртуозных профессионалов по кибербезопасности

- Экспертные тренинги
- SOC Consulting
- Adversary Attack Emulation

Penetration Testing от Kaspersky поможет вам и вашей организации:

1

Определить самые слабые места в вашей сети, чтобы принять полностью обоснованные решения о том, куда лучше направить свое внимание и бюджет, а также снизить будущие риски.

2

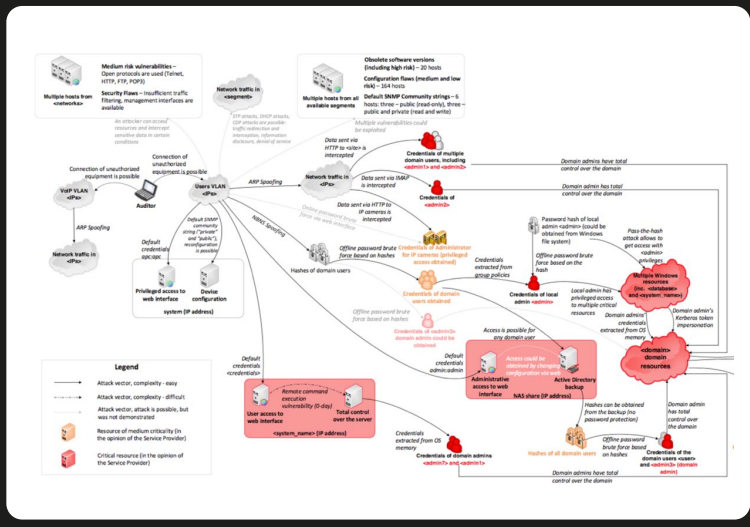
Избежать финансовых, операционных и репутационных потерь, вызванных кибератаками, путем предотвращения атак за счет проактивного обнаружения и устранения уязвимостей

3

Соответствовать государственным, отраслевым или внутренним корпоративным стандартам, требующим проведения подобной оценки безопасности (например, PCI DSS).

Высокоуровневое резюме и подробные технические отчеты для обоснования приоритетных мер по исправлению ситуации

- Оценка уровня безопасности
- Обзор перспектив нападения
- Индикаторы атак и компрометации
- Визуализация векторов атак
- Краткосрочные, среднесрочные и долгосрочные рекомендации
- Описание уязвимостей и ошибок в конфигурации

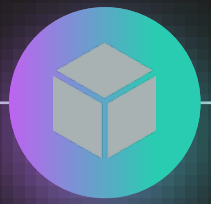


Анализ защищенности приложений – Методология оценки безопасности приложений

Black Box

Оценка без учетных данных пользователя для выявления уязвимостей, доступных внешнему злоумышленнику без каких-либо привилегий

- Нулевое знание
- Испытание в роли атакующего



Grey Box

Выявление уязвимостей, доступных пользователям. Для анализа необходимо предоставить тестовые учетные записи пользователей

- Некоторые знания
- Тестирование в качестве пользователя с доступом к некоторым данным

White Box

Анализ исходного кода и архитектуры. Оценка безопасности White Box позволяет выявить максимально возможное количество уязвимостей

- Полное знание
- Тестирование в качестве разработчика

Kaspersky Application Security Assessment помогает в:

Предотвращении финансовых, операционных и репутационных потерь за счет упреждающего обнаружения и устранения уязвимостей, используемых в атаках на приложения.

Экономии затрат на устранение последствий благодаря обнаружению уязвимостей в приложениях, находящихся на стадии разработки и тестирования, до того, как они попадут в пользовательскую среду, где их устранение может привести к значительным сбоям и затратам.

Поддержке безопасного жизненного цикла разработки программного обеспечения

Соблюдении государственных, отраслевых и внутренних корпоративных стандартов, таких как GDPR или PCI DSS.

Предварительная работа

Black box / grey box оценка

White box оценка

Эксплуатация

Отчетность и рекомендации

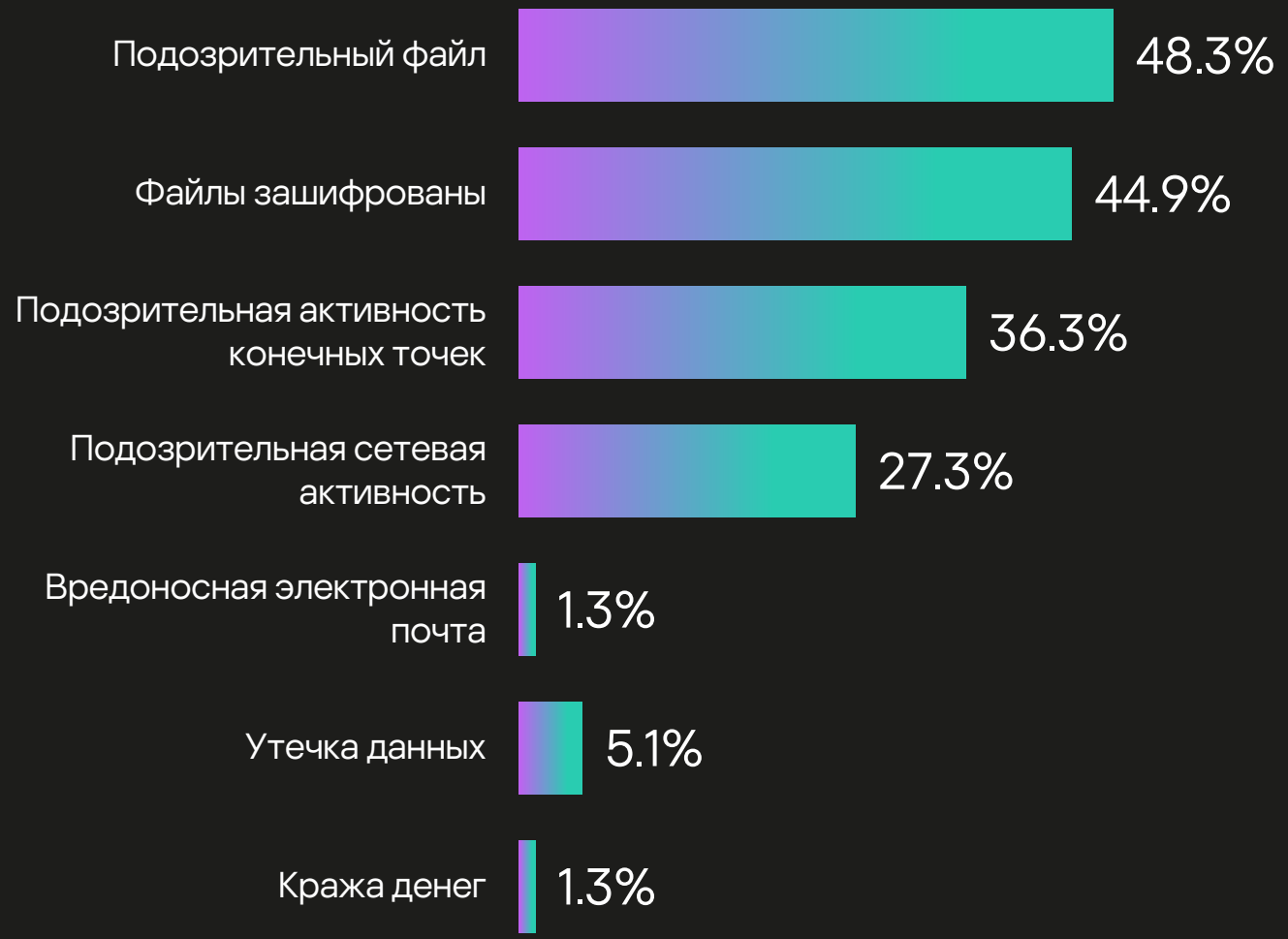
Проверка устранения недостатков

Penetration Testing vs. Red Teaming

	Penetration Testing	Red Teaming
Основные цели	Обнаружить как можно больше уязвимостей, продемонстрировав доступ к критически важным активам	Моделирование поведения противника при уклонении от обнаружения, чтобы проверить реакцию защищающейся стороны
Ограничения	Строгие рамки, этические нормы и временные рамки	На основе модели угроз - по умолчанию нет
Результаты	Список уязвимостей, рекомендации по устранению	Выводы по оборонительным возможностям, рекомендации по улучшению
Цена	Умеренная	Высокая

Причины обращения за услугами по реагированию на инциденты

Заметные последствия для инфраструктуры, такие как зашифрованные активы, потеря денег, утечка данных или подозрительные электронные письма, привели к 30 % запросов на расследование. Более 50 % запросов поступило от оповещений в инструментальных системах безопасности: конечных (EPP, EDR), сетевых (NTA) и других (FW, IDS/ IPS и т. д.).



Kaspersky Incident Response

Реагирование на инциденты - это услуга по расследованию, которая позволяет воссоздать подробную картину инцидента. Услуга охватывает полный цикл расследования и реагирования на инцидент, начиная с раннего реагирования на инцидент и сбора доказательств на месте и заканчивая выявлением дополнительных следов компрометации и разработкой рекомендаций по устранению последствий.

Сервис отвечает на такие вопросы, как

- Что произошло?
- Кто был целью атаки?
- Когда это произошло?

Инцидент

Сбор улик

Анализ

Отчет

Преимущества

1

Сводит к минимуму сбои в работе и затраты на простои

2

Сохраняет отношения и доверие с вашими клиентами

3

Дополняет вашу команду специалистами по первому требованию

4

Обеспечивает непрерывное совершенствование системы безопасности

5

Помогает избежать значительных штрафов и пеней

6

Обеспечивает обмен знаниями с внутренней командой

Удаленно

- Анализ улик
- Подготовка отчета

На месте

- Ликвидация последствий
- Сбор улик

Экстренная помощь

IR Retainer

- Стандартное SLA
- Без повторного использования

IR Retainer Premium

- Расширенный SLA
- Перепрофилирование в сервисы Threat Intelligence: APT Reports, Threat Lookup, Cloud Sandbox, Threat Data Feeds

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

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.

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.

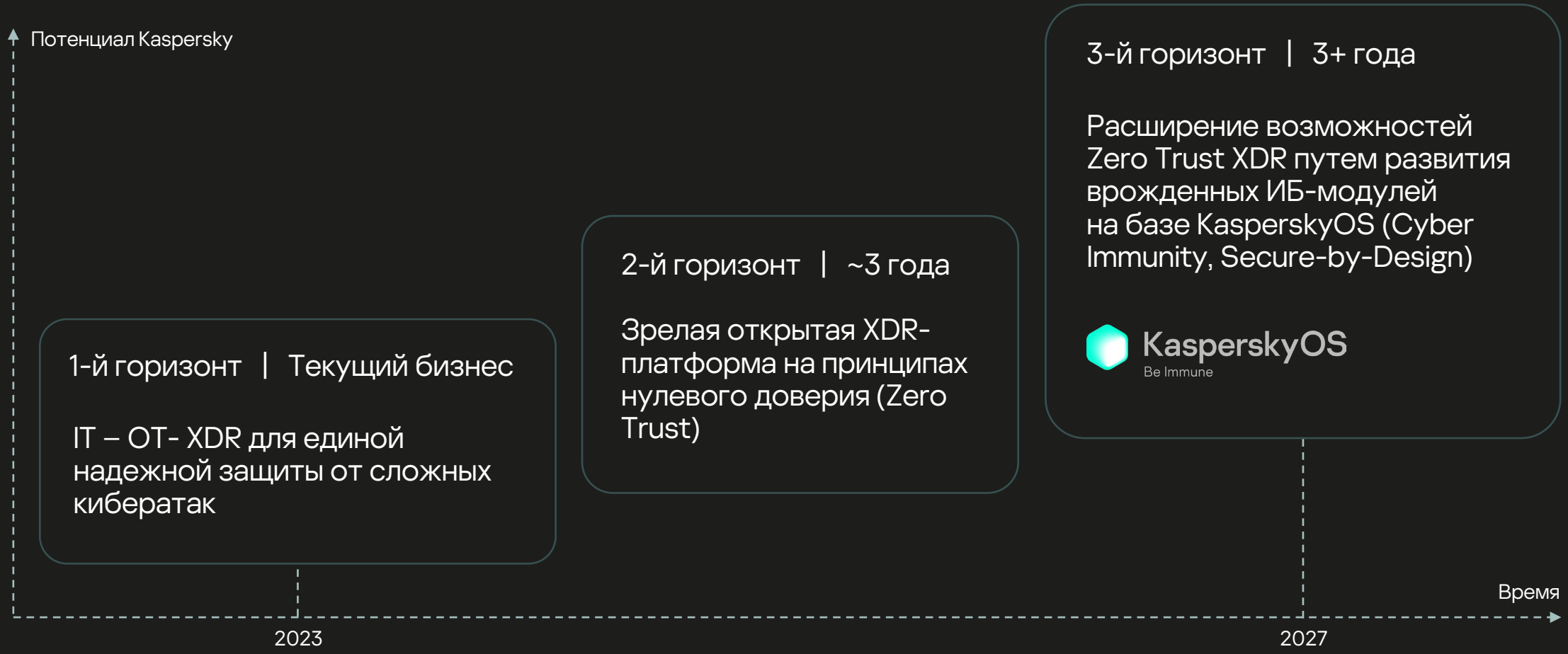
ISO / IEC 27001

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.

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