26.11.2024

Кибербезопасность конфиденциальных медицинских данных

Алексей Киселев,
руководитель отдела
по работе с клиентами
среднего и малого бизнеса
«Лаборатория
Касперского»

Усложнение рисков

Технологический суверенитет

Поиск актуальных решений

Интерактивная карта киберугроз

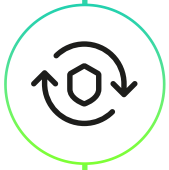
Подробнее

Напряженный киберландшафт

В последние два года 69% организаций в России пострадали минимум от одного киберинцидента.

Усложнение регулирования

Обсуждается существенное увеличение штрафов за утечки.



Технологический суверенитет

Продолжается активное замещение иностранных защитных ИБ решений, покинувших российский рынок. Повышаются требования регуляторов.

Ландшафт киберугроз

+39% рост количества критических инцидентов в организациях России и СНГ (Q1 2024 VS Q1 2023)

>2 инцидентов высокой критичности ежедневно

>19 млн паролей российских пользователей обнаружены в даркнете в Q1 2024 (x6 по сравнению с Q1 2023)

Здравоохранение – в топ-5 отраслей по количеству утечек в 2023

Самые распространенные причины: нарушение политики безопасности, целевые кибератаки, вредоносное ПО

Основная угроза для организаций – по-прежнему шифровальщики. В 2023 году с ними был связан каждый третий инцидент

Аналитический отчет Kaspersky Managed Detection and Response за 2023 год; Отчет «О значимых утечках данных в России» от команды Kaspersky Digital Footprint Intelligence,

Утечки данных

Общие сведения о значимых[1] утечках данных в российских компаниях в 2023 году[2]:

133

факта утечек данных за 2023 год

За 2022 год	За 2023 год
141 факт утечек данных	133 факта утечек данных
>230 млн пользовательских данных	>310 млн пользовательских данных
>33 млн записей с паролями	>47 млн записей с паролями

47 976 727

Строк, содержащих парольную информацию, было скомпрометировано злоумышленниками

В каких сферах были самые крупные утечки?

- 4 Ритейл
- 2 Финансы
- 1 Интернет-сервисы
- 1 Здоровье
- 1 Карьера и образование
- 1 Производство

Подробнее

Отчет «Значимые утечки в 2023 году»

Утечки данных

Топ-5 пострадавших отраслей от утечек данных

2022	2023
Ритейл	Ритейл
↓ Рестораны и доставки еды	↑ Интернет-сервисы
Интернет-сервисы	↑ Финансы
Карьера и образование	Карьера и образование
↓ Транспорт	↑ IT

Топ-5 отраслей по объемам скомпрометированных данных

2022	2023
Доставка	↑ Ритейл
СМИ	↑ Финансы
Ритейл	↑ Интернет-сервисы
Здоровье	↑ Карьера и образование
Социальные сети	↓ Здоровье

Подробнее

- **Начало 2024**: Роскомнадзор сообщил об **одном** инциденте с компрометацией **500 млн** записей о россиянах

- **Январь 2024:** утечка данных пользователей Rendez-Vous: **7,6 млн** уникальных номеров и **4,5 млн** e-mail-адресов

- **Март 2024:** утечка базы сети ортопедических салонов «Ортека»: **3,8 млн** уникальных номеров и **428 тыс.** e-mail-адресов

- **Март 2024:** Минцифры Казахстана зафиксировало утечку персональных данных казахстанского МФО. В обнаруженном файле также содержались данные клиентов российских МФО, функционирующих на платформе Robo.finance: в общей сложности **>23,6 млн данных клиентов из России**.

Регулирование в области защиты персональных данных (ПДн)

Нормативная база:

- **Федеральный закон РФ № 152-ФЗ «О персональных данных»**
- **Приказ Роскомнадзора от 14.11.2022 N 187**
  порядок взаимодействия операторов с Роскомнадзором в случае инцидентов в области ПДн
- **Приказ ФСБ России от 13.02.2023 N 77**
  порядок взаимодействия операторов с ГосСОПКА
- **Приказ ФСТЭК России от 18.02.2013 N 21**
  комплекс мер для построения эффективной системы информационной безопасности

+ связанные документы.

Подробнее

Ответственность за нарушения в области защиты ПДн

Сегодня: административная ответственность

Невыполнение оператором при сборе данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения или извлечения персональных данных граждан.

Физлицо: штраф **до 100 000 руб.**
Юрлицо: штраф **до 18 млн руб.**
Должностное лицо: штраф **до 800 000 руб.**

Использование несертифицированных информационных систем, баз и банков данных, средств защиты информации.

Физлицо: штраф **до 2 500 руб.**
Юрлицо: штраф **до 25 000 руб.**
Должностное лицо: штраф **до 3 000 руб.**

Нарушение требований о защите информации.

Физлицо: штраф **до 1 000 руб.**
Юрлицо: штраф **до 15 000 руб.**
Должностное лицо: штраф **до 2 000 руб.**

Перспектива: оборотный штраф и уголовная ответственность

Усиление ответственности за нарушение порядка обработки ПДн (законопроект принят Госдумой в первом чтении).

Невыполнение оператором обязанности по уведомлению Роскомнадзора в случае установления факта неправомерной передачи ПДн, повлекшей нарушение прав субъектов ПДн.

Физлицо: штраф **до 100 000 руб.**
Юрлицо: штраф **до 3 млн руб.**
Должностное лицо: штраф **до 800 000 руб.**

Действия (бездействие) оператора, повлекшие неправомерную передачу информации.

Физлицо: штраф **до 400 тыс руб.**
Юрлицо: штраф **до 15 млн руб.**
Должностное лицо: штраф **до 2 млн руб.**

Оборотные штрафы для компаний, допустивших утечку личной информации граждан – **до 3% выручки** (за повторное нарушение).

Использование, передача, сбор и хранение ПнД, полученных незаконным путём, создание информационных ресурсов, распространяющих такие данные. **Лишение свободы — до 10 лет**.

Генная инженерия

Регенеративная медицина

Нанотехнологии

Вмешательство в технологии – УГРОЗА ЖИЗНИ

Безопасность данных

Медицинские данные поистине бесценны – ведь от них зависят человеческие жизни. Связанные с ними технологии можно разделить на две категории.

Имплантируемые технологии

Устройства интернета вещей и другие жизненно необходимые имплантаты для мониторинга состояния здоровья или лечения (например, кардиостимуляторы)

Технологии работы с клиническими данными

Имеют дело с огромным потоком информации, возникающей в результате взаимодействия пациента с системой здравоохранения

Подлинность данных

Медицинская карта – это набор конфиденциальной информации, который исключительно подробно описывает жизнь человека.

Не только кража

Риски, которые возникают, если к ней получат доступ киберпреступники, не ограничиваются обычной кражей персональных данных (даже с учетом революции биометрической идентификации)

Фальсификация

Может представлять смертельную опасность – подлинность данных становится в прямом смысле вопросом жизни и смерти

Доступность данных

Работникам здравоохранения, имеющим дело с пациентами, может быть сложнее осваивать инновации, чем офисным сотрудникам.

Программы - вымогатели

Атака WannaCry на Национальную службу здравоохранения Великобритании, атака SamSam на поставщика ПО для управления здравоохранением Allscripts

DDoS-атаки

Атака на сеть правительства Новосибирской области – деградировали медицинская информационная система и колл-центр)

Нарушители внутри организации

Здравоохранение является единственной отраслью, где утечки чаще происходят по вине внутренних, а не внешних злоумышленников.

Огромное число многопользовательских учетных записей

К корпоративным сетям организаций здравоохранения имеет доступ множество самых разных лиц, включая подрядчиков и рядовых сотрудников

Отсутствие строгих политик доступа и необученность персонала

Обмен картами доступа, пароль на мониторе…

Мобильные медицинские устройства и интернет вещей

Только за последний год количество уязвимостей в медицинских устройствах выросло на 525%.

Больше функционала – больше угроз

Медицинские приложения отслеживают все данные – от режима питания до циклов фертильности и сна, притягательность этой сферы для преступников и уровень угрозы для пользователей наверняка продолжат возрастать в геометрической прогрессии

Как мы можем помочь

3 СЛОЖНЫЕ АТАКИ

Kaspersky Expert Security

Служба ИБ или SOC

- Повышение экспертизы: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky EDR Expert; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack
- Реагирование на угрозы: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

2 СКРЫТЫЕ УГРОЗЫ

Kaspersky Optimum Security

Команда ИБ

- Базовое обнаружение и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Песочница: Kaspersky Sandbox
- Обогащение данными: Kaspersky Threat Intelligence Portal
- Киберграмотность: Kaspersky Security Awarenes s
- Защита контейнеров: Kaspersky Container Security
- Умная защита для среднего бизнеса: Kaspersky Smart

1 МАССОВЫЕ УГРОЗЫ

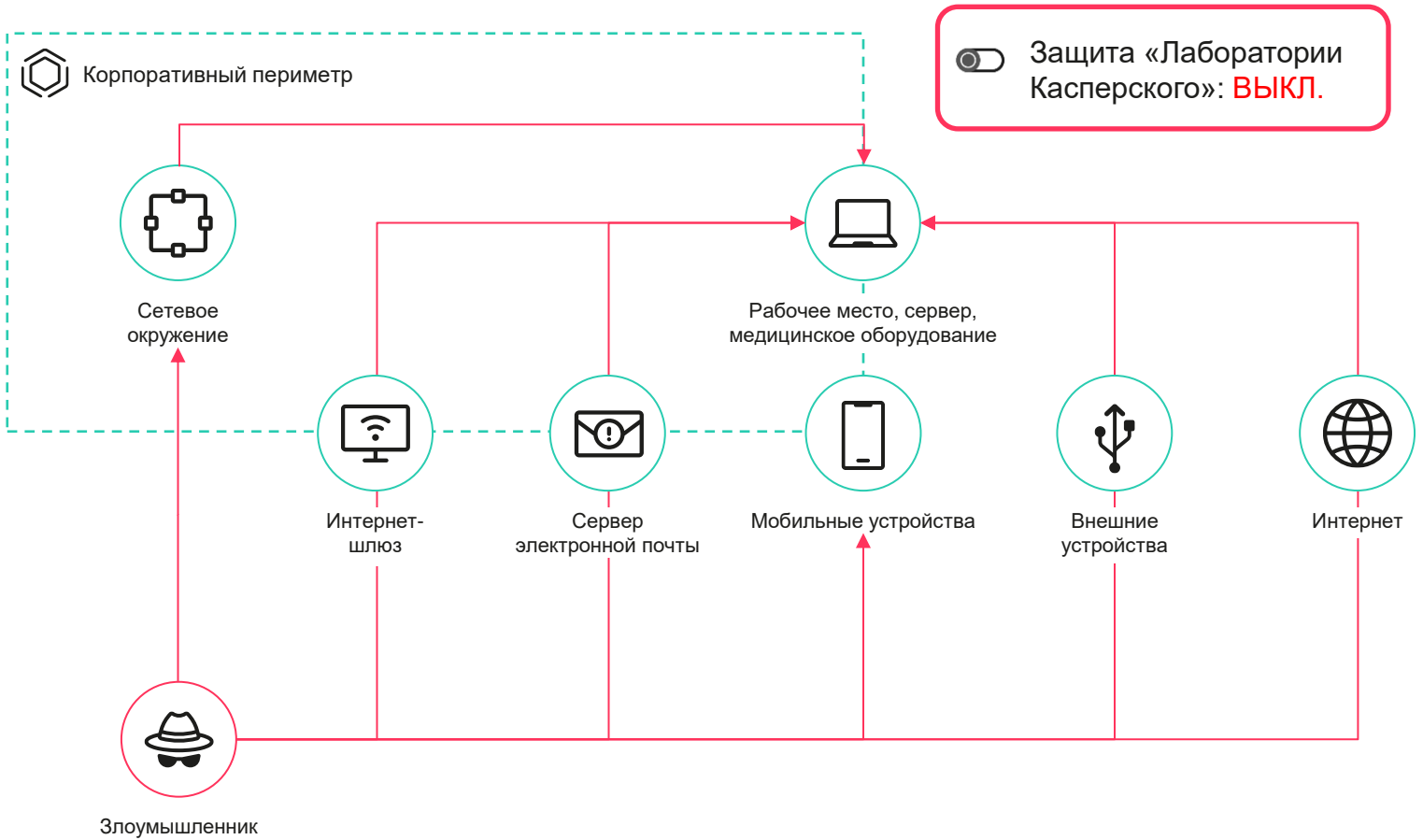
Kaspersky Security Foundations

ИТ

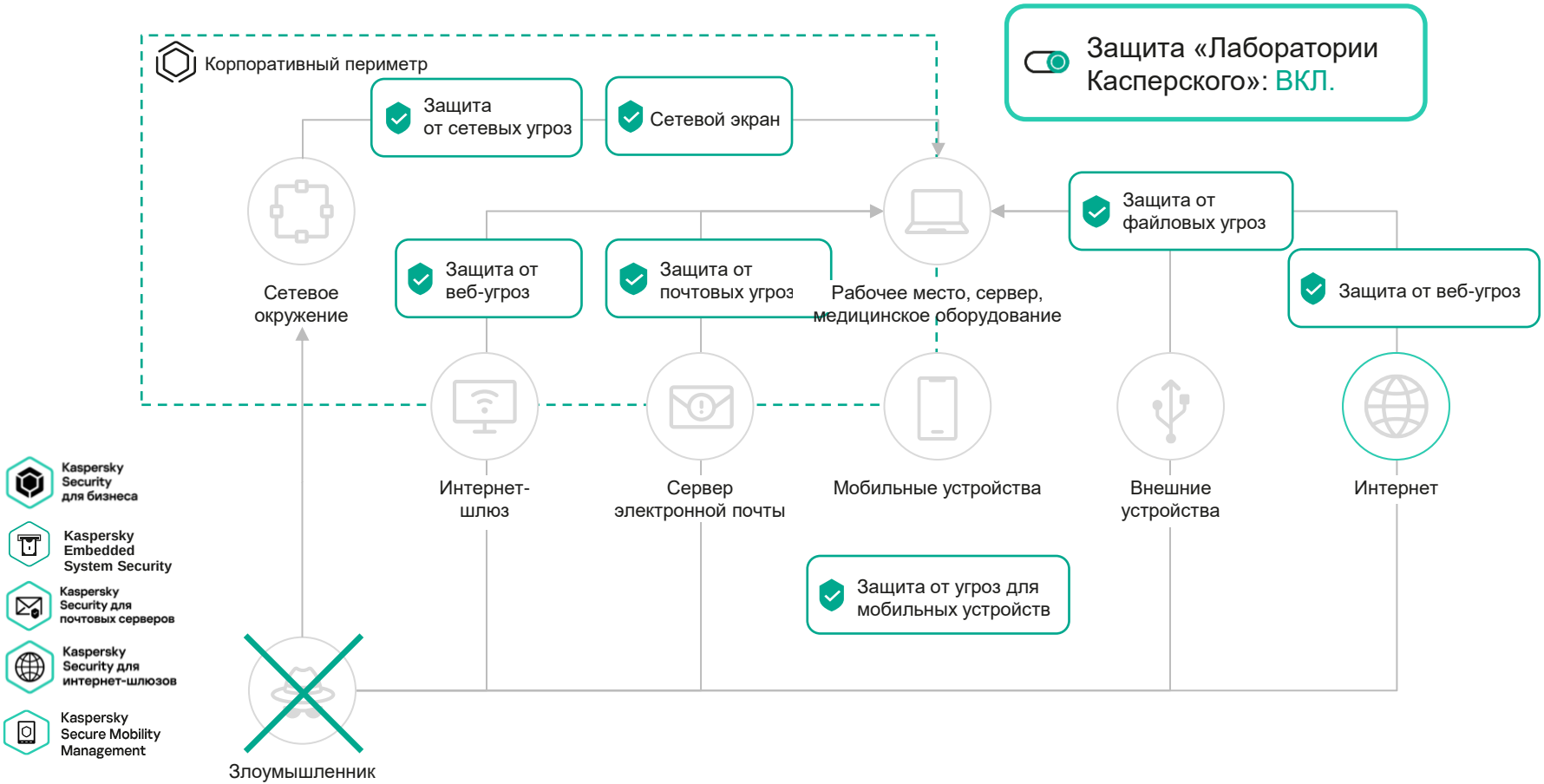
- Конечные устройства: Kaspersky Security для бизнеса; Kaspersky Embedded System Security; Kaspersky Security для виртуальных и облачных сред; Kaspersky Secure Mobility Management
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security для интернет-шлюзов
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: MSA и профессиональные сервисы

Kaspersky Managed Detection and Response

Что защищать в первую очередь

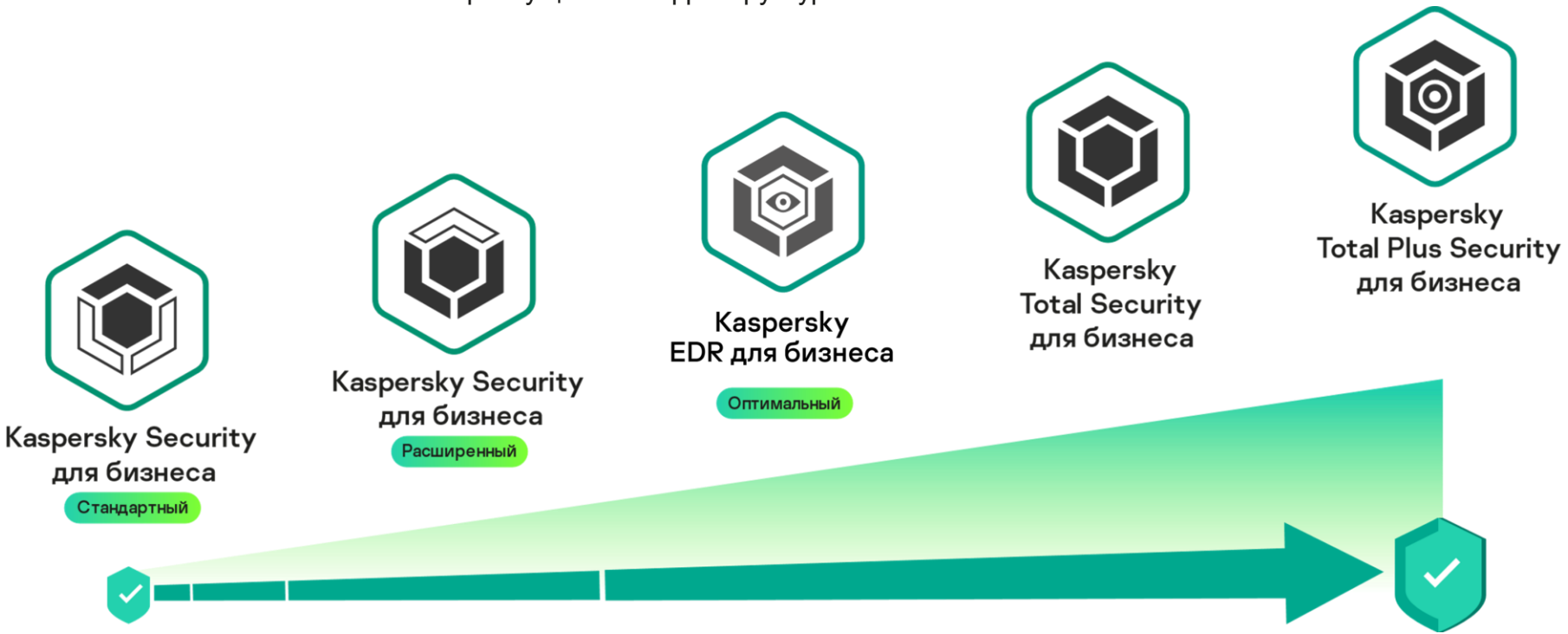


Базовая защита на всех подступах к инфраструктуре



Мы предлагаем несколько уровней защиты

На каждом уровне технологии сбалансированы так, чтобы удовлетворить любые потребности, связанные с безопасностью вашей растущей IT-инфраструктуры.



О продукте

Специализированное решение для защиты встраиваемых систем (банкоматы,
POS-системы, торговые автоматы, заправочные станции, медицинское оборудование) от угроз любого типа и любой сложности

Ключевые возможности

- Укрепление системы (контроль безопасности)
- Дополнительная защита от вредоносного ПО: методы эвристического анализа и модели машинного
- Защита от эксплойтов
- Защита от сетевых угроз
- Контроль целостности и соблюдение нормативных требований
- Поддержка маломощных и устаревших систем
- Анализ журналов
- Гибкое управление – локально или в облаке
- Управление сетевым экраном
- Эффективная защита даже при нестабильном подключении к сети

О продукте

Позволяет бизнесу безопасно, гибко и удобно использовать мобильные устройства в рабочих целях. Уверенный контроль и надежная защита на каждом этапе жизненного цикла корпоративных мобильных устройств

Ключевые возможности

- Простое управление всем парком мобильных устройств и централизованное управление политиками из единой консоли
- Поддержка всех основных сценариев использования устройста (COPO, COBE, BYOD)
- Управление устройствами Android, iOS/IPadOS и жизненным циклом Windows-устройств
- Надежная защита устройств в том числе от специализированных мобильных угроз
- Корпоративный каталог приложений
- Управление и работа с сертификатами и VPN (per-app VPN)
- Полная поддержка режима supervised для iOS и возможностей в нем

Kaspersky Secure Mobility Management

О продукте

Позволяет бизнесу безопасно, гибко и удобно использовать мобильные устройства в рабочих целях. Уверенный контроль и надежная защита на каждом этапе жизненного цикла корпоративных мобильных устройств

Подробнее

Подготовка

- Развертывание сервисов поддержки мобильной платформы (серверная часть)
- Подготовка корпоративного каталога со списком доверенных приложений и портала для подключения BYOD-устройств
- Подготовка и конфигурирование сценариев автоматизированного развертывания корпоративных устройств

Развертывание и конфигурация

- Загрузка сертификатов безопасности, профилей email, VPN, Wi-Fi
- Установка агентской части решения, обеспечивающей защиту устройств и функции мониторинга/контроля
- Загрузка и применение корпоративных политик безопасности и ограничений использования
- Установка и автоматизированное конфигурирование бизнес-приложений

Защита и контроль

- Отслеживание событий безопасности
- Реагирование на события уровня «инцидент», включающее вмешательство администратора
- Отслеживание и реагирование на события регуляторных политик

Поддержка и выведение из обслуживания

- Обеспечение удаленной поддержки
- Аудит потерянных / украденных устройств
- Отзыв доступа к корпоративным ресурсам
- Выборочное (для BYOD-устройств) или полное обнуление устройства

О продукте

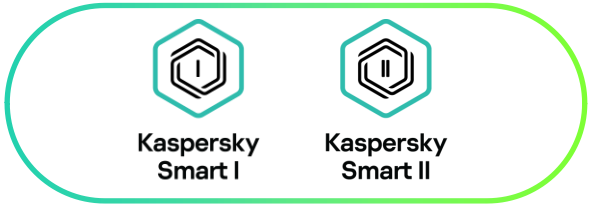
Kaspersky DDoS Protection минимизирует влияние DDoS-атак, обеспечивая постоянную доступность всей инфраструктуры и важнейших онлайн-ресурсов.

Подробнее

Ключевые возможности

Все необходимое для защиты от любых видов DDoS-атак и уменьшения их последствий:

- **Анализ трафика в режиме 24x7x365**
  Уникальная сенсорная технология для анализа трафика в реальном времени
- **Географически распределенные центры очистки**
  Масштабируемые и отказоустойчивые центры очистки
- **Безупречная интеграция** без необходимости покупки дополнительного оборудования
- **Гибкость решения**. Постоянное перенаправление трафика или перенаправление по требованию
- **Надежная поддержка**. Эксперты «Лаборатории Касперского» круглосуточно отслеживают аномалии в трафике клиентов



О продукте

Линейка решений Kaspersky Smart делает экспертные инструменты класса SIEM и MDR доступными для организаций среднего бизнеса (250–1000 узлов) и открывает новые возможности для киберзащиты.

Подробнее

Ключевые возможности

Kaspersky Smart I

SIEM

Kaspersky Smart II

SIEM EDR

- Единая поставка самой актуальной киберзащиты для среднего размера инфраструктур
- Не только мониторинг и обнаружение, но и реагирование
- Помощь в соблюдении требований регуляторов
- Комплексная защита организаций среднего размера с минимальными требованиями к аппаратным мощностям и возможностью установки на виртуальные машины

Акция на покупку Kaspersky Smart. До 31 декабря 2024

Скидка на покупку

15 %

Kaspersky Smart I

30 %

Kaspersky Smart II

Kaspersky Automated Security Awareness Platform

О продукте

Платформе для обучения сотрудников основам кибербезопасности. Простой и эффективный онлайн-инструмент, который поможет сотрудникам овладеть навыками кибербезопасного поведения и применять их в работе

Подробнее

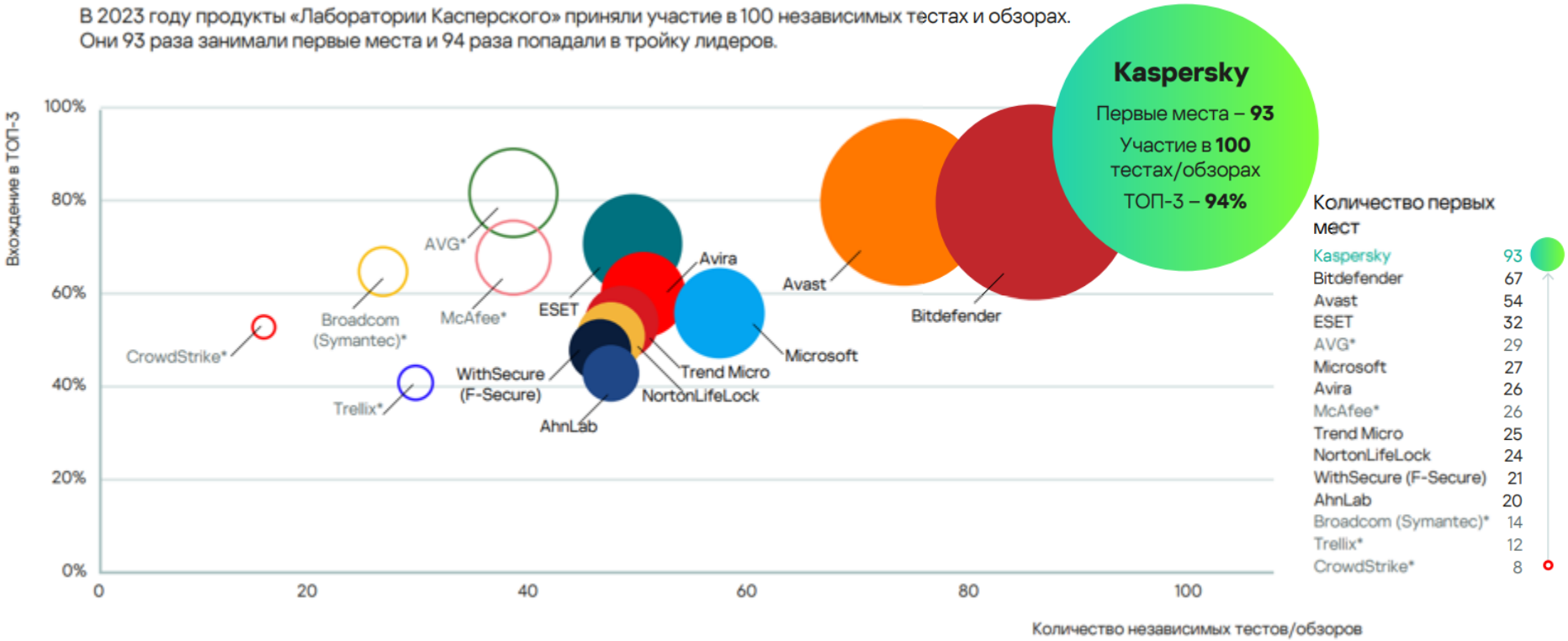
Ключевые преимущества

- Снижение числа инцидентов, связанных с человеческой ошибкой;
- Повышение квалификации сотрудников в области кибербезопасности;
- Соответствие требованиям регуляторов в отношении киберграмотности сотрудников;
- Автоматизация процессов, экономия времени сотрудников IT по управлению тренингом и отслеживанию прогресса;
- Простота и удобство использования;
- Контент, покрывающий все основные темы ИБ, включая ИИ и кибербезопасность промышленных систем.

Скидка на покупку 35 %

До 31.12.2024

Подтвержденное лидерство



Переход с зарубежных решений. Программа «Мигрируй»

1

Выгода

Получите скидку до 40% на покупку лицензии при переходе на Kaspersky с решений других вендоров.

2

Предоставьте лицензию

Предоставьте авторизованному партнеру Kaspersky копию лицензионного соглашения.

Мигрируй!

Подробнее

Спасибо за внимание!

Алексей Киселев
Alexey.Kiselev@Kaspersky.com

kaspersky