08.04.2025

Кибербезопасность

Обоснование инвестиций в ИБ

Алексей Киселев

Руководитель отдела продаж клиентам
малого и среднего бизнеса
«Лаборатории Касперского»

kaspersky

Неопределенность. Больше рисков. Поиск решения.

Усложнение киберландшафта

В первом полугодии 2024 года в России и СНГ количество критичных киберинцидентов выросло на 39% по сравнению с аналогичным периодом 2023 года*

Киберагрессия

Более 126 миллионов киберугроз были обнаружены и заблокированы «Лабораторией Касперского» на устройствах российских пользователей в 2023 году.

Доля российских пользователей, которые потенциально могли пострадать от этих атак, составляет 45,43%

Атаки на цепочки поставок

В 2023 и 2024 году кибератаки через подрядчиков входят в тройку самых распространенных векторов, и в 2025 году эта тенденция продолжится.

* Добавить ссылку

Тренды 2025

Рост числа атак на цепочки поставок

Важность обеспечения безопасности Linux

Расширение альянсов хактивистов

Изобретательные фишинговые атаки на B2B

Более активное применение ИИ в кибератаках

Атаки на цепочки поставок

Ущерб от атак на цепочку поставок может быть значительным — от простоев и нарушения бизнес-процессов до репутационных рисков и срывов контрактов с ключевыми заказчиками.

Этот тип атак характеризуется тем, что злоумышленники получают доступ к инфраструктуре компании через ее поставщиков или поставляемое программное обеспечение.

Предотвратить подобные атаки крайне непросто — ведь значительная часть действий злоумышленников происходят в инфраструктуре, которая неподконтрольна ИБ-службе.

Все компании, независимо от размера, могут стать объектом атаки потому, что они взаимодействуют с очень крупными организациями, но не обладают эшелонированной защитой и являются слабым звеном к крупной цели.

Рост атак на Linux

Количество вредоносных файлов для Linux (в нашей коллекции)

За последние пять лет количество атак на Linux-устройства увеличилось более чем

в 20 раз

- Вымогатели
- Майнеры
- Уязвимости
- Вредоносное ПО для IoT
- Атаки, проводимые операторами

Угрозы и решения

Массовые	Скрытые	Продвинутые
Наиболее распространены	Легко найти в даркнете	Часто – целевые атаки
Простое обнаружение	Избегают обнаружения	Сложны в обнаружении
Легко устраняются	Значительные последствия	Многовекторные и устойчивые

Решение

- Базовая защита: защита «периметра»: конечных точек, серверов, почты, интернет-шлюзов, управление корпоративной мобильностью
- Усиление защиты (system hardening)

- Выделенные сотрудники ИБ
- Технологии и экспертиза для обнаружения и реагирования

- Продвинутые технологии обнаружения, реагирования, расследования мониторинга и анализа данных по всей инфраструктуре: EDR, NDR, SIEM, XDR
- Глубокая ИБ-экспертиза

Как обосновать инвестиции в ИБ?

Возражения

Кибератака может
не произойти, а деньги будут
потрачены

Продемонстрируйте измеримые
результаты
от потенциального внедрения

Простой ответ

Уровень финансовых потерь
в случае успешной кибератаки
вероятнее всего превысит сумму
требуемых инвестиций. А глядя на
текущий ландшафт угроз, сложно
представить, что компании без
надёжной защиты удастся избежать
инцидентов.

Три понятных подхода к обоснованию инвестиций в кибербезопасность

1

Анализ рисков

2

Анализ временных затрат

3

Требования регуляторов

Потери бизнеса*

>$200k в год – средние потери одной российской компании, пострадавшей от киберугроз.

Формула расчета окупаемости инвестиций в ИБ (ROI):

$$\frac{\text{Возможный материальный ущерб} - \text{Совокупная стоимость владения}}{\text{Совокупная стоимость владения}} \times 100\%$$

Последствия целевой атаки для организации

- Компрометация данных
- Ухудшение репутации
- Утрата критически важных данных
- Кража денежных средств
- Кража коммерческой тайны
- Потеря конкурентного преимущества
- Повреждение ИТ-инфраструктуры
- Утрата доверия клиентов
- Прерывание основных бизнес-процессов
- Уменьшение занимаемой доли на рынке
- Недоступность сервисов для пользователей
- Прямые и косвенные денежные потери

* По разным оценкам

Анализ временных затрат

Время

Самый дефицитный ресурс при расследовании инцидентов и реагировании на инциденты. Он представляет из себя сумму двух критериев.

Mean Time to Detect (MTTD)

1

Время обнаружения

Среднее время, необходимое организации для обнаружения нарушения безопасности или угрозы

2

Mean Time to Respond (MTTR)

Время реагирования

Среднее время, необходимое на реакцию и устранение обнаруженной угрозы

Анализ временных затрат

Факторы, увеличивающие длительность инцидента

- Выполнения сложных задач в условиях нехватки квалифицированных кадров и экспертизы
- Ручной разбор и анализ большого числа инцидентов
- Эксплуатации средств ИБ, которые не взаимодействуют друг с другом и управляются из разных консолей
- Принятия решений без использования средств наглядного централизованного представления информации

Факторы, сокращающие длительность инцидента

- Наличие передовых эффективных технологий защиты
- Автоматизация ИБ-процессов и экономия ресурсов ИБ-специалистов
- Единая платформа кибербезопасности с синхронизированными решениями и средствами управления

39 минут

Среднее время обнаружения сложных угроз в рамках сервиса Kaspersky MDR

40–46 часов

Среднее время реагирования на разные типы атак, согласно отчету Kaspersky Incident Response

Анализ временных затрат

Формулы расчета времени, которое понадобится аналитикам для разрешения одного инцидента (без средств автоматизации)

1

При использовании сторонних услуг по реагированию на инцидент

Затраты на разрешение одного инцидента = Время на разрешение инцидента × Стомость услуги по реагированию на инцидент

2

При самостоятельном реагировании на инцидент без помощи специализированных средств

Затраты на разрешение одного инцидента = Время на разрешение инцидента × Стоимость нормо-часа аналитика × Количество требуемых аналитиков

Рассчитайте затраты на разрешение инцидентов

Для проведения дальнейших расчетов по возможным затратам на разрешение инцидентов, можно взять три усредненных варианта суммарного времени разрешения инцидента без использования специализированных средств, учитывая в том числе возможное разнообразие атак, с которыми могут столкнуться организации:

- 15 дней
- 30 дней
- 90 дней

Определенные требования регуляторов обязательны для выполнения. При их невыполнении возможны прямые убытки.

Пример:

Повторное нарушение, связанное с утечкой персональных данных, влечет
за собой — оборотный штраф — от 1% до 3% от выручки
за предшествующий календарный год, но не менее 25 млн и не более 500 млн ₽.

Ключевые аспекты современных законодательных требований

Только отечественные решения

Полный запрет для ряда организаций использования СЗИ и сервисов по информационной безопасности, происходящих из недружественных стран.

Указ Президента РФ от 01.05.2022 N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Сертифицированное ПО

Использование решений, присутствующих в Реестре российского ПО Минцифры РФ и имеющего сертификаты ФСБ и ФСТЭК России, в т.ч. в цепочке поставок.

Проверка инфраструктуры

на наличие получаемых от регуляторов (в т.ч. отраслевых) индикаторов компрометации, проведение оперативных мер по реагированию и пр.

Ключевые аспекты современных законодательных требований

Сбор и централизованное хранение данных,

вердиктов и иной информации, связанной с произошедшими инцидентами, которые позволяют оказывать содействие специалистам ФСБ, предоставляя им необходимую информацию об обнаруженных угрозах.

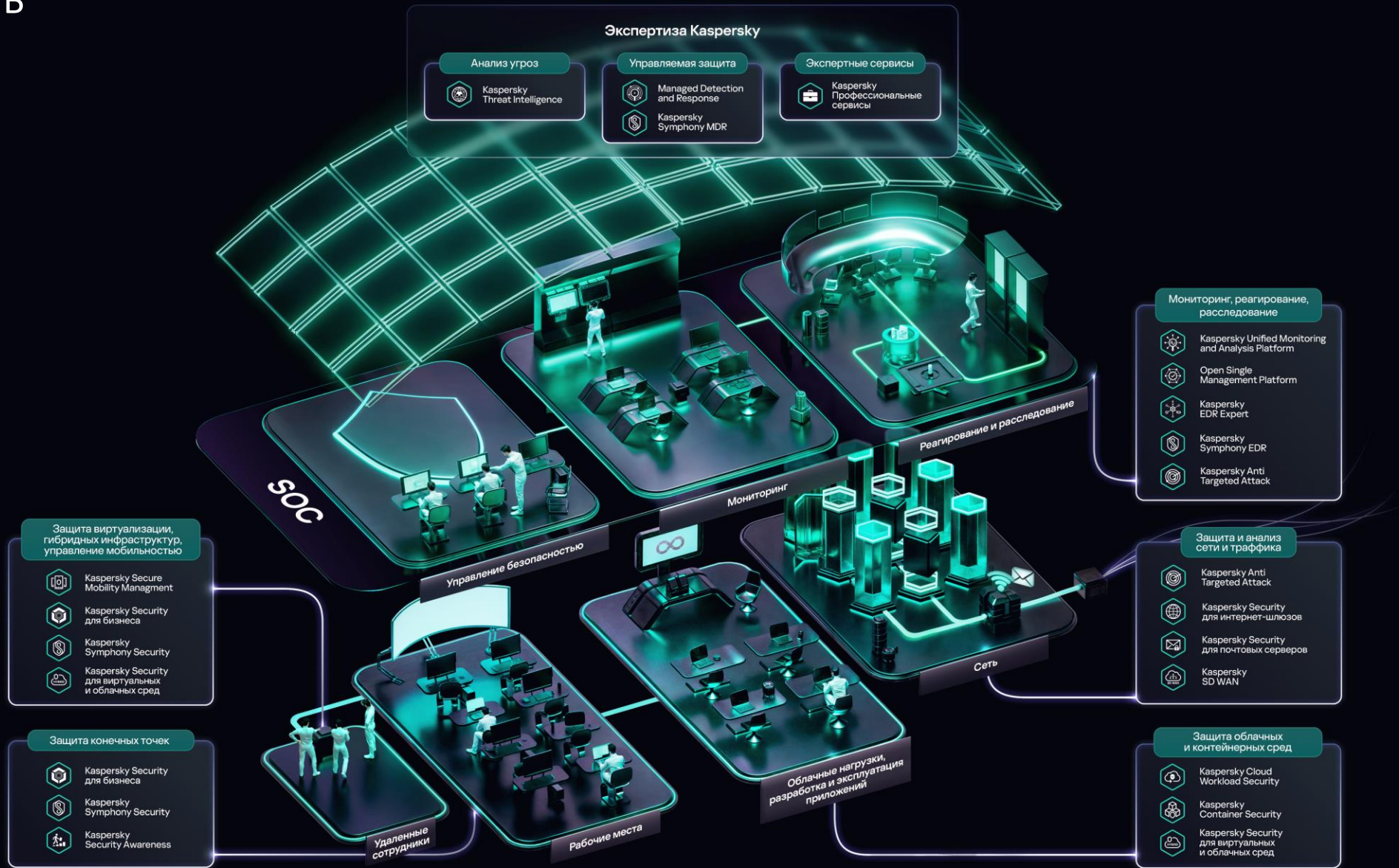
Обязательства по информированию

об инцидентах через передачу информации о кибератаках на КИИ в ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак).

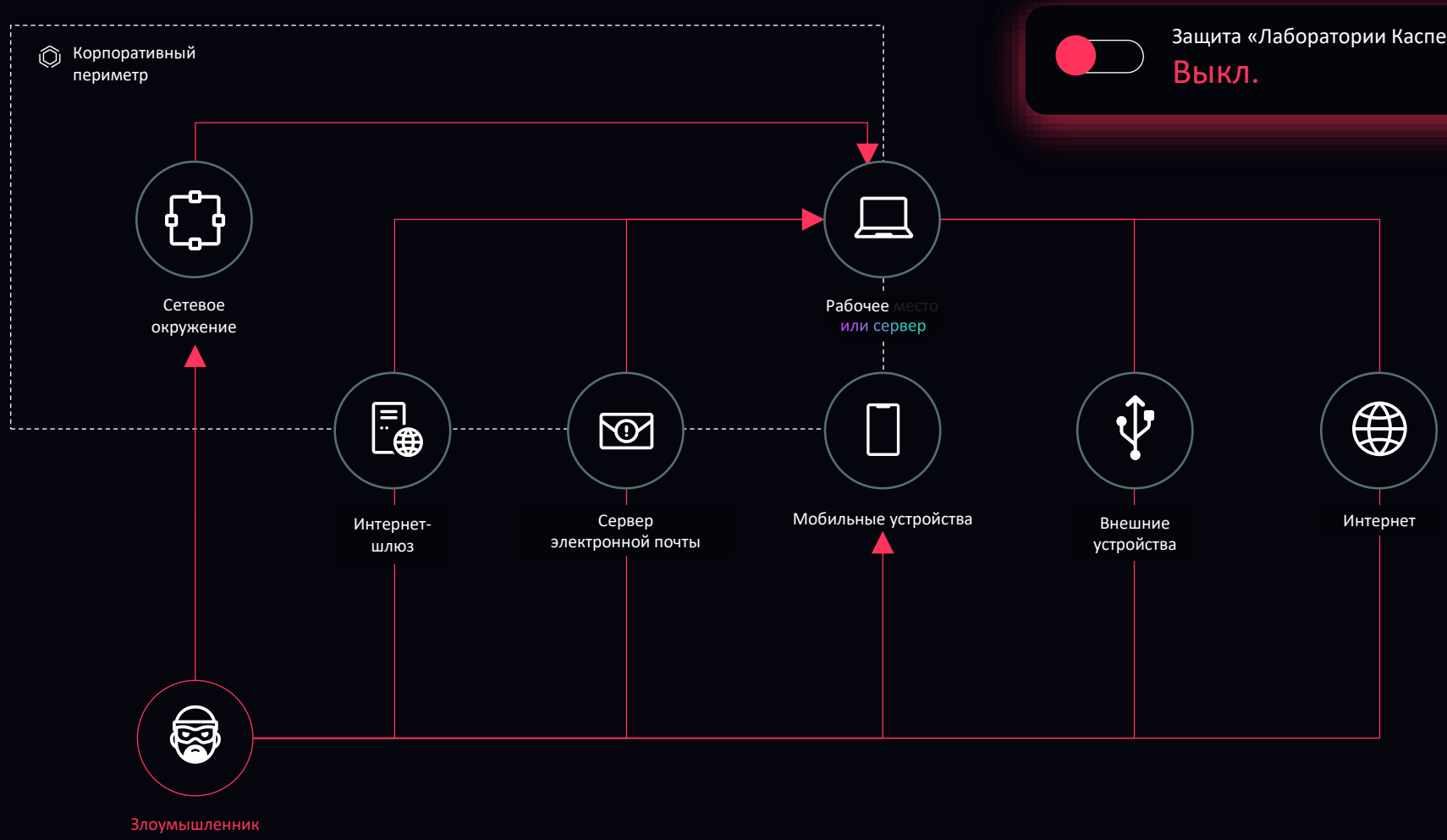
Защита персональных данных

Соблюдение требований по сбору, хранению ПДн, обращению с ними и их защите.

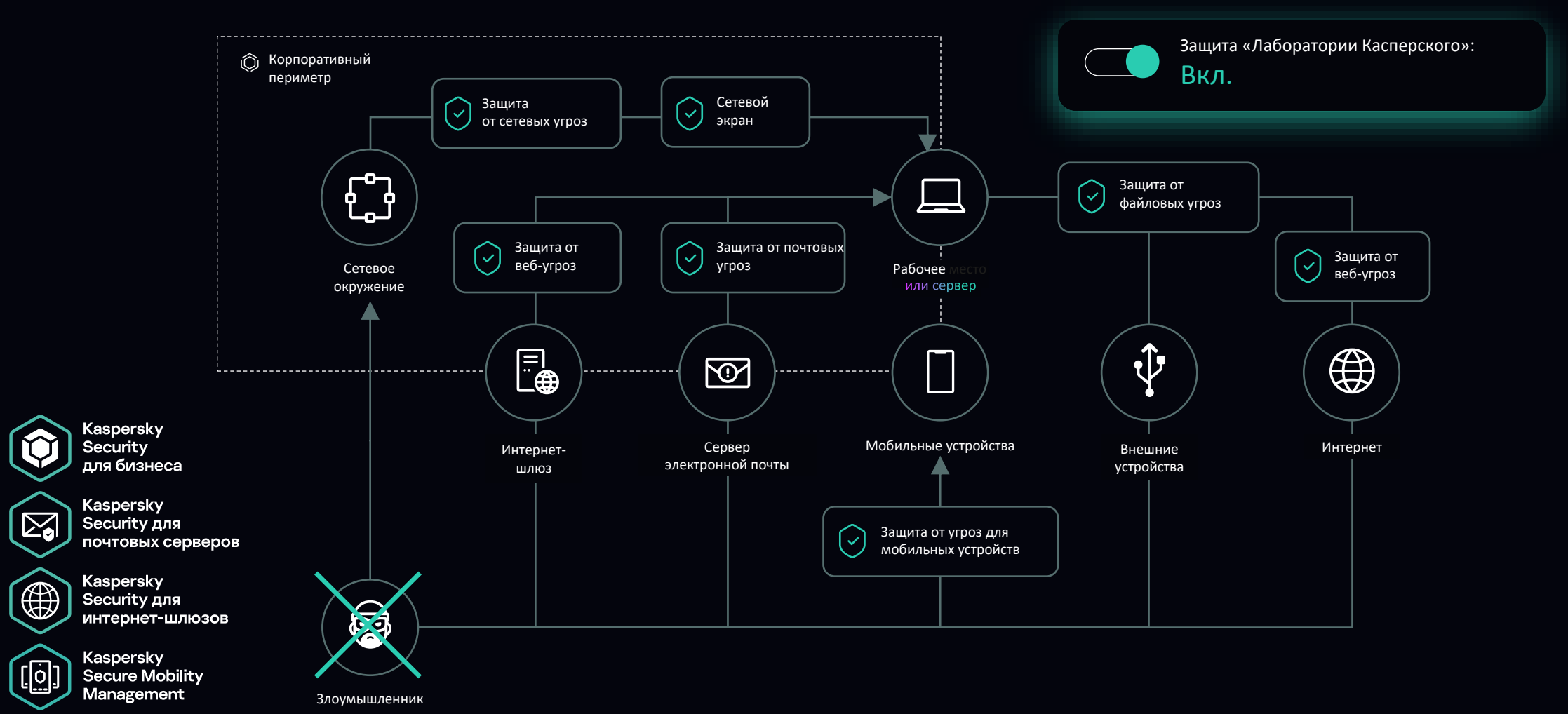
Платформа ИБ



Что защищать в первую очередь



Базовая защита на всех подступах к инфраструктуре



Управляемая защита (MDR)

Kaspersky Managed Detection and Response

Kaspersky Symphony MDR

Непрерывный поиск, обнаружение и устранение угроз, направленных на ваше предприятие

Ключевые возможности

- Проактивный поиск угроз (Threat Hunting)
- Обзор всех защищаемых ресурсов с их текущим статусом REST API для интеграции с IRP / SOAR
- Прямой доступ к аналитикам SOC по вопросам инцидентов
- Консоль управления с панелями мониторинга и отчетами
- Совместимость со сторонними антивирусными решениями
- Хранение необработанной телеметрии в течение 3 месяцев
- Возможность самостоятельно зарегистрировать инцидент при подозрении на компрометацию
- Автоматическое и управляемое реагирование на инциденты
- Включенная защитой класса EPP – в Kaspersky Symphony MDR

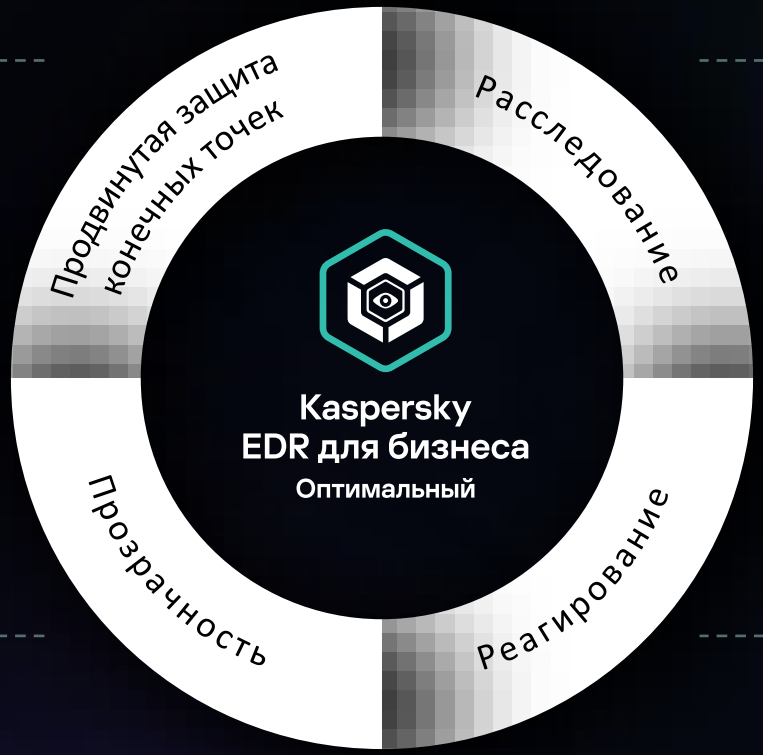
- Сокращение расходов на ИБ-персонал, возможность направить внутренние ресурсы на решение стратегических ИБ-задач

  Стоимость владения в год на 150 нод ≈ стоимость одного сотрудника*

* Точная стоимость всегда рассчитывается индивидуально

Решения-лайфхаки. Базовый EDR: Kaspersky EDR для бизнеса Оптимальный

- Поддержка всех основных платформ: Windows, MacOS, Linux
- Защита от новейших угроз, в том числе от бесфайловых вирусов
- Адаптивный контроль аномалий
- Автоматическое устранение угроз



- Анализ первопричин
- Детали по инциденту
- Обогащение данными Threat Intelligence

- Визуализация пути атаки
- Сканирование индикаторов компрометации
- Единая карточка обнаружения

- Рекомендации по реагированию
- Реагирование «в одно нажатие» и автоматическое реагирование
- Сетевая изоляция, запрет запуска, карантин

Выводы

1. Лучше потратить время на сложную аргументацию необходимости инвестиций, чем принимать решение по итогам пропущенного инцидента

2. Кибербезопасность – это процесс

3. Платформенная кибербезопасность – современный тренд, отвечающий потребностям рынка

Спасибо за внимание!

Алексей Киселев

Alexey.Kiselev@Kaspersky.com