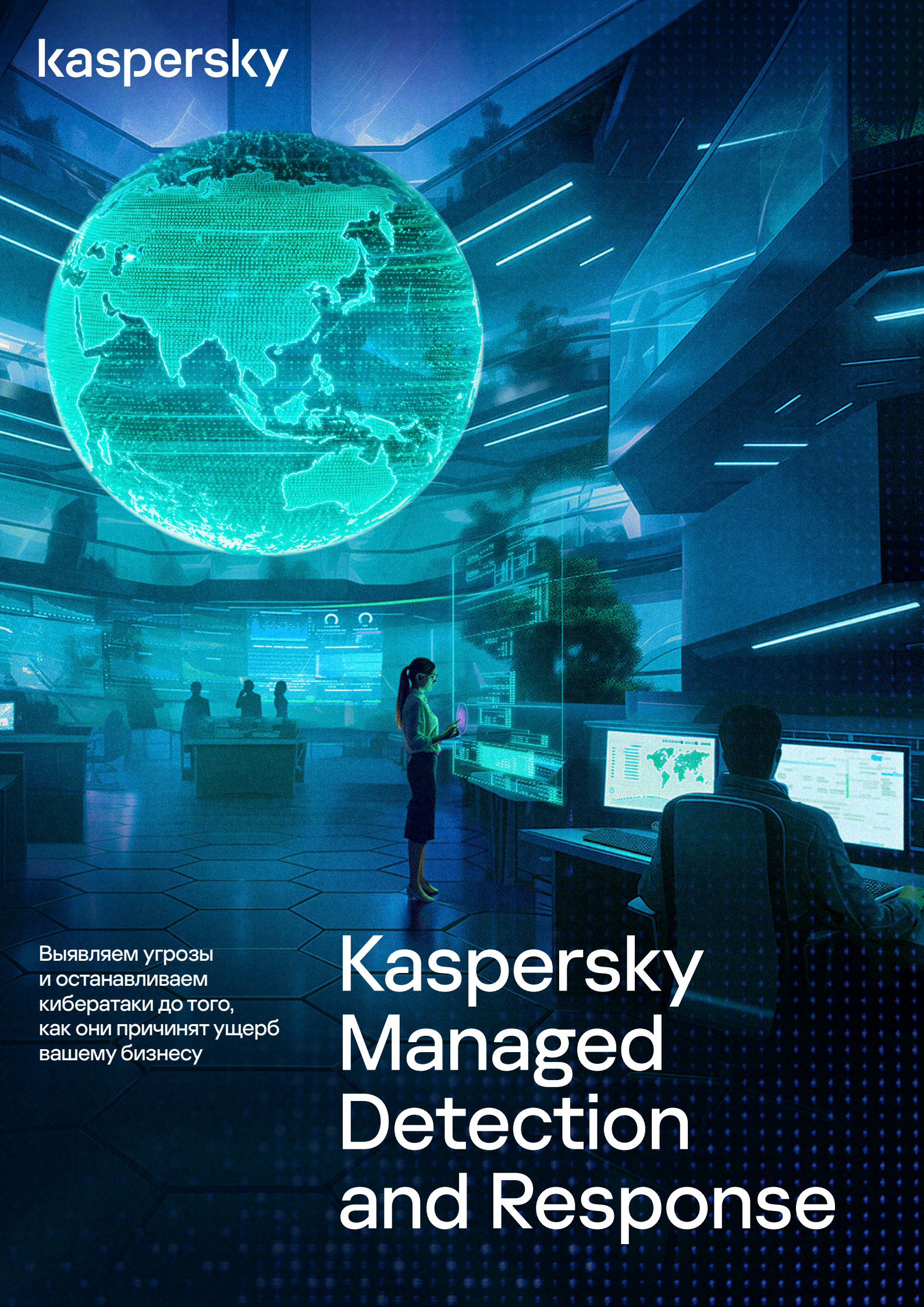
kaspersky



Выявляем угрозы
и останавливаем
кибератаки до того,
как они причинят ущерб
вашему бизнесу

Kaspersky Managed Detection and Response

Повысьте надежность своей системы кибербезопасности с помощью круглосуточной управляемой защиты

На организации любого масштаба постоянно оказывают давление такие факторы, как удаленная работа, быстрорастущий объем цифровых данных, усиливающаяся нехватка квалифицированных кадров, а также увеличение числа киберугроз, способных обходить традиционные автоматизированные средства защиты. В этих условиях крайне важно быстро и эффективно реагировать на все инциденты

Kaspersky Managed Detection and Response – это экспертный сервис для круглосуточного мониторинга, обнаружения и расследования сложных кибератак и быстрого реагирования на них. Позволяет усилить существующие средства защиты благодаря обнаружению угроз силами экспертов «Лаборатории Касперского», использованию глобальной аналитики об угрозах и функций ИИ Автоаналитика. Сервис позволяет повысить уровень безопасности OT- и ИТ-инфраструктур вне зависимости от размера организации и сферы ее деятельности.

Обзор современных киберугроз[1]

1 Начальные векторы атак

44%
Компрометация через доверительные отношения

25%
Легитимные учетные записи

16%
Эксплуатация уязвимостей в публичных приложениях

2 Действия в инфраструктуре

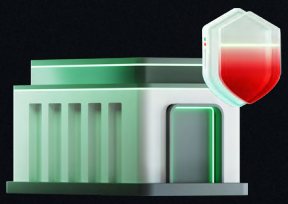
Злоумышленники часто используют легитимные инструменты (такие как Ngrok, PsExec, SoftPerfect Network Scanner) в инфраструктурах, где отсутствует надлежащий контроль за конфигурацией системы.

3 Ущерб

39%
зашифрованных файлов

12%
закрепление в системе для будущих атак

7%
эксфильтрация через веб-сервис



Факты свидетельствуют о том, что злоумышленники часто возвращаются после проведения успешной атаки.

Длительность атаки

Быстрая	Среднесрочная	Длительная
51%	16%	33%
в пределах одного дня	19 дней	108 дней

Ключевые преимущества

Постоянная расширенная защита по всей поверхности атаки – на рабочих местах, в сети, облачных средах и других компонентах инфраструктуры – с первого дня использования.

Готовый круглосуточно работающий центр мониторинга и реагирования без затрат на создание и поддержку собственного SOC.

Снижение нагрузки на ваших ИБ-специалистов: функции мониторинга, первичной оценки и расследования угроз передаются нам.

Безопасность, ориентированная на результат: сочетание экспертизы наших специалистов, аналитики угроз и ИИ-технологий позволяет останавливать инциденты ещё до того, как они нанесут ущерб вашему бизнесу.

> Благодаря внедрению решения мы смогли снять часть задач с наших сотрудников и передать их центру SOC «Лаборатории Касперского», а это значительная экономия ресурсов при улучшении качества мониторинга событий безопасности.

Большой театр

Максим Иванов,
начальник отдела ИТ, телефонной связи и телевидения службы связи ИТиТСБ «Государственного академического Большого театра России»

Подробнее

1 Глобальный отчет Kaspersky Security Services о ландшафте киберугроз, 2026.

Возможности Kaspersky MDR

Непрерывная защита от комплексных угроз сразу после внедрения

Kaspersky MDR активируется за несколько минут и не требует дополнительной инфраструктуры. Благодаря нашим специалистам из центра мониторинга и реагирования, а также аналитике угроз обеспечивается многоуровневое обнаружение угроз по всей инфраструктуре. Благодаря анализу множества сигналов телеметрии сервис проактивно обнаруживает угрозы, выявляет первопричины инцидентов и обеспечивает оперативное реагирование на них, защищая организацию от известных и неизвестных угроз с первого дня работы.

Управление безопасностью под руководством экспертов с использованием данных аналитики

При использовании сервиса Kaspersky MDR безопасность вашей организации поддерживают международные эксперты с большим практическим опытом работы, имеющие престижные отраслевые сертификаты. Работа экспертов дополняется лучшими на рынке технологиями аналитики угроз и искусственного интеллекта – они встроены в сервис и позволяют повысить точность и контекстность оповещений, ускорить обнаружение угроз и сократить среднее время реагирования на инциденты (MTTR).

Эффективность работы и предсказуемость затрат

- Kaspersky MDR позволяет избежать сложностей и затрат, связанных с созданием собственного центра мониторинга и реагирования с нуля. Это помогает быстрее внедрять необходимые улучшения в области безопасности без значительного увеличения нагрузки на бюджет.
- Если у вас уже есть собственный центр мониторинга и реагирования, наш сервис возьмет на себя задачи по круглосуточному мониторингу, приоритизации оповещений и классификации инцидентов, чтобы разгрузить ваших аналитиков и позволить им сосредоточиться на критически важных задачах и развитии безопасности.

Сценарии использования

- Круглосуточная защита «под ключ» для организаций, не имеющих службы ИБ
- Совместная модель управления ИБ, позволяющая расширить возможности собственных специалистов по кибербезопасности
- Расширенная защита промышленной инфраструктуры
- Непрерывная специализированная защита встраиваемых систем

30 минут
среднее время реагирования на инцидент [2]

30%
всех полученных оповещений обрабатываются ИИ Автоаналитиком [1]

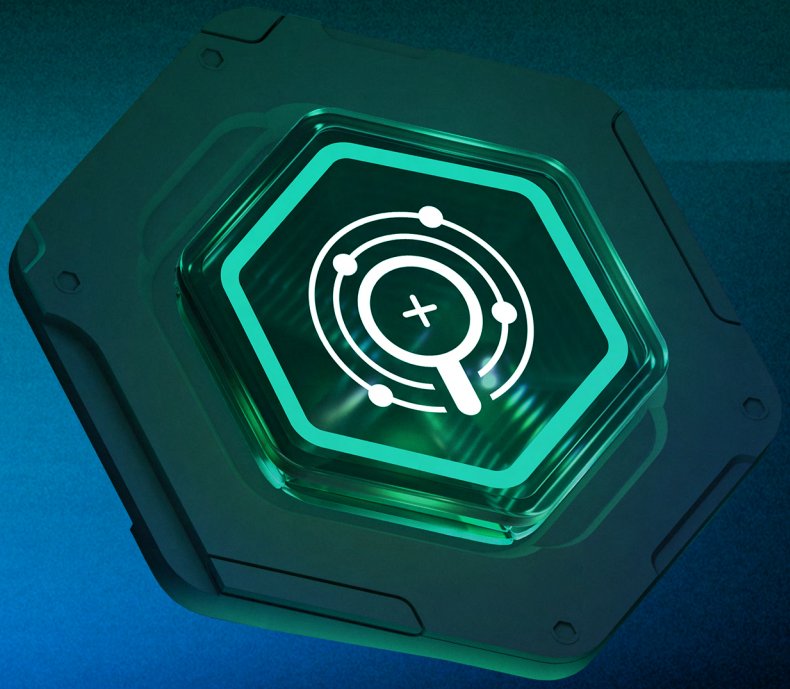
Около 5 минут
требуется на активацию сервиса Kaspersky MDR

До 2 лет
требуется на создание собственной службы ИБ с нуля

70%
специалистов по ИБ с трудом справляются с тем количеством оповещений, которое генерируется их средствами защиты [3]

2 Согласно нашим ежегодным аналитическим отчетам MDR

3 Портрет современного специалиста по информационной безопасности на 2024 год



Kaspersky Managed Detection and Response

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее