# Сравнение ключевых B2B-решений


kaspersky АКТИВИРУЙ БУДУЩЕЕ

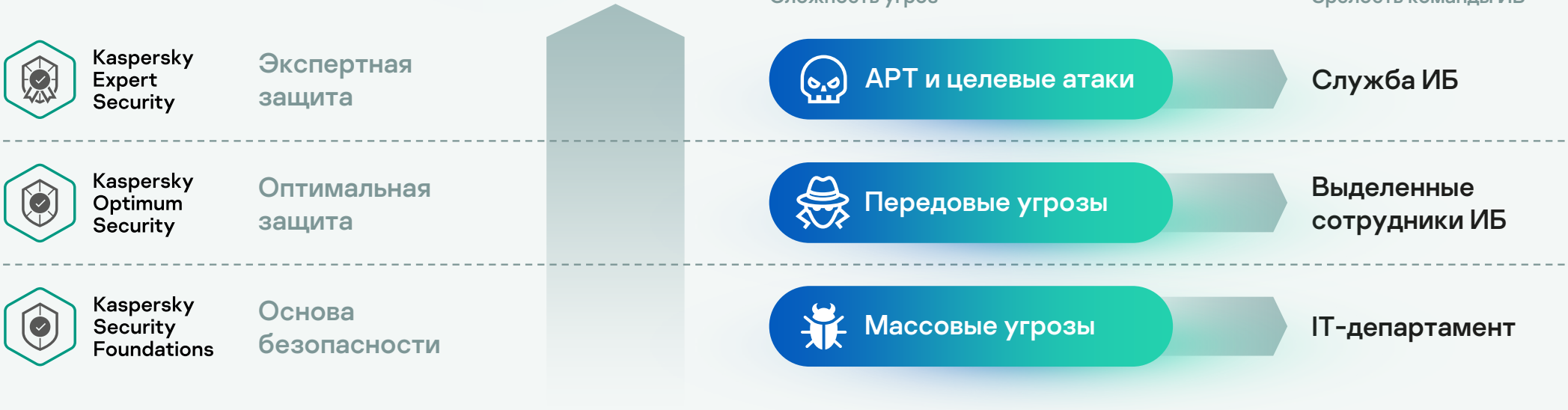
## Трехуровневая защита

Понимая взаимосвязь сложности киберугроз и требуемой экспертизы для их отражения, «Лаборатория Касперского» создала трехуровневый подход к построению стратегии защиты, основанный на многолетнем опыте и знании инструментов, которые киберпреступники используют при различных типах атак. Этот подход также учитывает степень зрелости корпоративной IT-безопасности.

# Защита для каждой компании

**Сегодня злоумышленники атакуют различные организации, независимо от их размеров, сферы деятельности и уровня готовности к отражению киберугроз. Эти угрозы и атаки, начиная с известных и неизвестных вредоносных программ, шифровальщиков, бесфайловых угроз и заканчивая APT-атаками и целевыми кампаниями, отличаются широким разнообразием в плане подходов, а также объема времени и усилий, которые киберпреступники в них вкладывают. Злоумышленники рационально используют свои силы и рассчитывают свои затраты исходя из планируемой выгоды. Очевидно, что на небольшие организации с базовым уровнем защиты не будут направлены дорогостоящие инструменты нападения — киберпреступнику будет достаточно отправить, например, фишинговое письмо с неизвестным вредоносным содержимым, чтобы получить «вознаграждение». А для атак на более крупные предприятия киберпреступники могут использовать весь арсенал инструментов, включая специально разработанное вредоносное ПО, которое умеет обходить традиционные средства защиты.**

Учитывая эти обстоятельства, **каждая компания должна быть в состоянии отражать направленные на нее современные киберугрозы разного уровня сложности**, даже в условиях нехватки персонала и глубоких знаний в области информационной безопасности. В некоторых организациях есть полноценные службы ИБ, обладающие необходимой квалификацией, другие могут вообще не иметь в штате специалистов по ИБ или же только начинать формирование собственного отдела ИБ.



В этом документе мы остановимся на ключевых элементах каждого уровня защиты от «Лаборатория Касперского» и проведем их функциональное сравнение.

Ключевым элементом базового уровня защиты Kaspersky Security Foundations является:

1

## Kaspersky Security Foundations

### Уровень первый

Основа безопасности для компаний любого размера и сферы деятельности. На этом уровне автоматически отражаются массовые киберугрозы, что позволяет удовлетворить потребности малых предприятий без выделенной группы ИБ, а также обеспечить более крупные компании фундаментом для перехода на следующий уровень защиты с вовлечением ИБ-экспертов.

Подробнее

## Kaspersky Endpoint Security для бизнеса

Расширенный

**Kaspersky Endpoint Security для бизнеса Расширенный** обеспечивает комплексную многоуровневую защиту корпоративной сети от известных, неизвестных и части передовых угроз. Уникальное сочетание аналитических данных, технологий машинного обучения и заложенного в технологиях опыта экспертов позволяет успешно предоставлять организациям любого размера и сферы деятельности автоматическую фундаментальную защиту от угроз.

# Kaspersky Optimum Security

## Уровень второй

Для небольших компаний с базовой ИБ-экспертизой или организаций, испытывающих недостаток ИБ-ресурсов. Уровень включает в себя на выбор: необходимый инструментарий для построения собственной системы защиты от передовых угроз или управляемую защиту силами экспертов «Лаборатории Касперского».

Ключевыми элементами оптимального уровня защиты Kaspersky Optimum Security являются:

1

Подробнее

### Kaspersky EDR для бизнеса Оптимальный

**Kaspersky EDR для бизнеса Оптимальный** объединяет технологии защиты рабочих мест и гибкие инструменты контроля, входящие в Kaspersky Endpoint Security для бизнеса Расширенный, с базовыми возможностями EDR (Endpoint Detection and Response), которые повышают прозрачность инфраструктуры рабочих мест, позволяют проводить анализ первопричин, работать с индикаторами компрометации (IoC) и оперативно реагировать на найденные угрозы.

2

Подробнее

### Kaspersky Managed Detection and Response Optimum

**Kaspersky MDR Optimum** — это интеллектуальный сервис управляемой безопасности, который максимально автоматизирован и основан на машинном обучении, но при этом находится под пристальным контролем экспертов «Лаборатории Касперского». Сервис мгновенно повышает уровень защиты от сложных угроз за счет быстрого развертывания услуги «под ключ». Kaspersky MDR Optimum подходит организациям с ограниченными ресурсами в области ИБ, обеспечивая круглосуточный мониторинг, обнаружение и приоритизацию инцидентов, а также помогая оперативно и точно на них реагировать.

# Kaspersky Expert Security

## Уровень третий

Подойдет для средних и крупных организаций, которые активно развивают свою внутреннюю ИБ-экспертизу, обеспокоены быстро усложняющимся ландшафтом угроз и понимают необходимость комплексной защиты от атак высокого уровня сложности.

Ключевыми элементами экспертного уровня защиты Kaspersky Expert Security являются:

1

## Kaspersky Endpoint Detection and Response

Подробнее

**Kaspersky EDR** — мощный экспертный EDR-инструмент в дополнение к Kaspersky Security для бизнеса или сторонним решениях класса EPP (Endpoint Protection Platform). Kaspersky EDR обеспечивает полный обзор всех рабочих мест в корпоративной сети и визуализацию каждой стадии расследования, предоставляет эффективное обнаружение, проактивный поиск киберугроз и расширенные возможности анализа первопричин. Процесс расследования подкрепляется ретроспективным анализом, а обнаружения сопоставляются с базой знаний MITRE ATT&CK.
С помощью Kaspersky EDR эксперты смогут воссоздать всю последовательность действий злоумышленников, обнаружить самые изощренные атаки и быстро принять эффективные контрмеры.

2

## Kaspersky Anti Targeted Attack

Подробнее

Платформа **Kaspersky Anti Targeted Attack**, усиленная возможностями Kaspersky EDR, обеспечивает передовую защиту от комплексных угроз и целевых атак в едином решении класса XDR (Extended Detection and Response). Полная визуализация происходящего в инфраструктуре, контроль всех популярных точек проникновения, возможность проведения анализа сетевого трафика а также эмуляция угроз при помощи продвинутой песочницы и мощные технологии EDR — все это делает процесс расследования и реагирования на инциденты более быстрым, точным и эффективным.

3

Подробнее

Kaspersky
Managed Detection
and Response
Expert

**Kaspersky MDR Expert** включает в себя все возможности Kaspersky MDR Optimum, а также предоставляет расширенную экспертизу и гибкость для опытных ИБ-команд. Крупные организации с развитой ИБ-экспертизой могут передать процессы классификации и расследования инцидентов в «Лабораторию Касперского» и направить свои ресурсы на решение более важных ИБ-задач. Kaspersky MDR Expert включает в себя доступ в портал Kaspersky Threat Lookup, проактивный поиск угроз силами экспертов «Лаборатории Касперского» для обнаружения тех инцидентов, по которым не было автоматических срабатываний, а также консультации аналитиков.

Подробнее

Kaspersky
Unified Monitoring
and Analysis Platform

Еще одно ключевое решение этого уровня — Kaspersky Unified Monitoring and Analysis Platform. Оно не включено в настоящее сравнение из-за того, что функциональность SIEM-систем кардинально отличается от рассматриваемых продуктов.

## Далее мы наглядно сравним функциональные возможности ключевых продуктов каждого из уровней.

# Сравнительная таблица решений

**Обозначения:**

- Входит в состав продукта
- Входит в состав продукта и содержит расширенные возможности
- Приобретается отдельно

## Функциональные возможности

| | Основа безопасности | Оптимальная защита | | Экспертная защита | | |
|---|---|---|---|---|---|---|
| | Kaspersky Security Foundations | Kaspersky Optimum Security | | Kaspersky Expert Security | | |
| | Kaspersky Endpoint Security для бизнеса Расширенный | Kaspersky EDR для бизнеса Оптимальный | Kaspersky Managed Detection and Response Optimum | Kaspersky Endpoint Detection and Response Advanced | Kaspersky Anti Targeted Attack с Kaspersky EDR | Kaspersky Managed Detection and Response Expert |
| Передовой антивирусный движок | ● | ● | | ○ | ○ | |
| Поведенческий анализ, защита от эксплойтов | ● | ● | | ○ | ○ | |
| Инструменты контроля и защита данных | ● | ● | | ○ | ○ | |
| Управление уязвимостями и обновлениями | ● | ● | | ○ | ○ | |
| Адаптивный контроль аномалий | ● | ● | | ○ | ○ | |
| Песочница | ○ | ○ | | ● | ● | |
| Обнаружение на основе IoC и пользовательских правил | | ● | | ● | ● | |
| Анализ первопричин | | ● | | ● | ● | |
| Поддержка различных мер по реагированию | | ● | | ● | ● | |
| Сбор и хранение «сырых» данных | | | | ● | ● | |
| Доступ к порталу Kaspersky Threat Lookup | | | | ● | ● | |
| Сопоставление с базой знаний MITRE ATT&CK | | | | ● | ● | |
| Расследование и реагирование на основе рекомендаций | | | | ● | ● | |
| Базовый инструментарий цифровой криминалистики | | | | ● | ● | |
| Проактивный поиск угроз и ретроспективный анализ | | | | ● | ● | |
| Анализ трафика | | | | | ● | |
| Передовое обнаружение почтовых и веб-угроз | | | | | ● | |
| Видимость на уровне сети и рабочих мест | | | | | ● | |
| Автоматическое реагирование на уровне шлюзов | | | | | ● | |
| | | | УПРАВЛЯЕМАЯ ЗАЩИТА ОПТИМАЛЬНОГО УРОВНЯ | | | УПРАВЛЯЕМАЯ ЗАЩИТА ЭКСПЕРТНОГО УРОВНЯ |

# Детальное сравнение уровней Kaspersky MDR

## Optimum

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанных данных в течение 1 месяца

Kaspersky Managed Detection and Response

## Expert

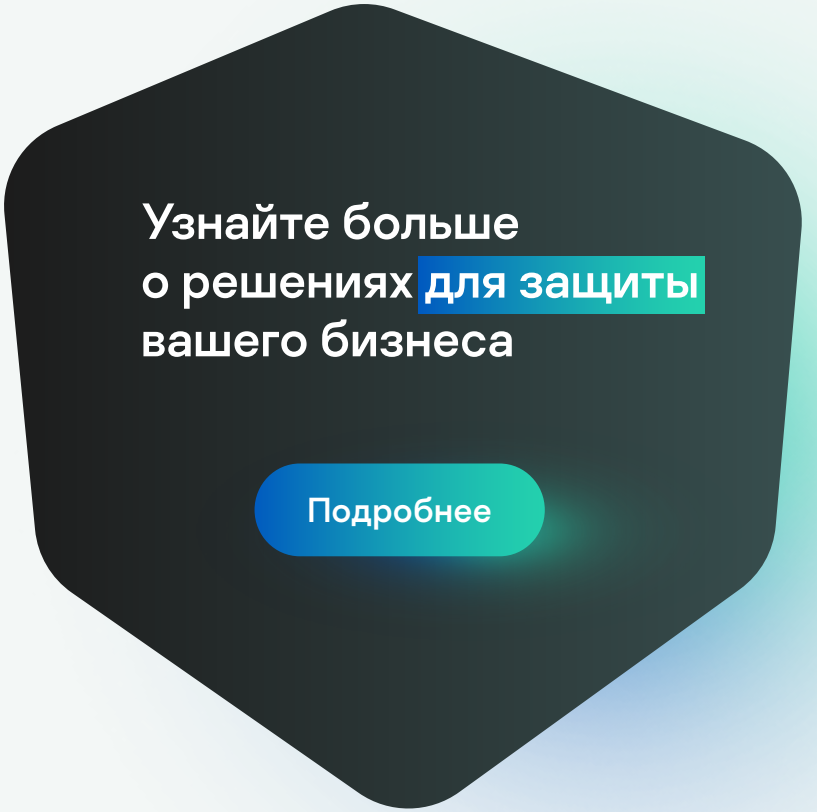
- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Сценарии реагирования и автоматическое реагирование на инциденты
- Обзор всех защищаемых ресурсов с их текущим статусом
- Единая консоль с панелями мониторинга и аналитическими отчетами
- Хранение истории инцидентов безопасности в течение 1 года

**ТОЛЬКО В EXPERT**

- Хранение необработанных данных в течение 3 месяцев
- Проактивный поиск угроз (threat hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Доступ к порталу Kaspersky Threat Lookup
- API для загрузки данных

# О подходе «Лаборатории Касперского»

**В портфолио «Лаборатории Касперского» имеется широкий спектр продуктов и сервисов, ориентированных на противодействие угрозам различного уровня сложности и отвечающих потребностям компаний разного размера и сфер деятельности. Наш подход призван помочь потенциальным клиентам в выборе наиболее подходящего решения для противодействия направленным на них угрозам, исходя из степени готовности к их отражению, а также имеющихся ресурсов, знаний и опыта.**




**www.kaspersky.ru**