



# **Kaspersky Expert Security: сложные и целевые угрозы – под вашим контролем**

## Крупные финансовые потери

Средний финансовый ущерб от утечки данных для крупных предприятий в 2020 году:



**\$1.092 m**

Источник: отчет IT Security Economics 2020, «Лаборатория Касперского»

# Kaspersky Expert Security

Ландшафт угроз постоянно меняется и быстро развивается. Всё больше организаций становятся жертвами многоэтапных целевых или АРТ-атак, которые могут привести к тяжелым последствиям. Если вы еще не сталкивались со сложными угрозами, будьте уверены – это всего лишь вопрос времени. Скоро ваши ИБ-специалисты окажутся лицом к лицу с киберугрозами нового поколения.

## Вы готовы к этому?

Для успешной борьбы с киберпреступниками необходимо наладить четкий процесс расследования инцидентов и реагирования на них, развивать экспертизу ИБ-специалистов и максимально эффективно использовать время и ресурсы.



## Kaspersky Expert Security

**Kaspersky Expert Security** позволяет вам взять под контроль сложные угрозы и построить эффективную экосистему информационной безопасности. Мы предлагаем интегрированные между собой продукты для противодействия сложным атакам, экспертную поддержку и тренинги для повышения квалификации ваших ИБ-специалистов.

## Почему кибератаки завершаются успехом?

### Недооценка угроз

Игнорирование вероятности сложной атаки. Внедрение продвинутой защиты только после серьезного инцидента.

### Неэффективные методы

Неупорядоченные и неэффективные методы работы с инцидентами в сочетании с разрозненными инструментами и слабой аналитикой угроз.

### Отсутствие поддержки

Отсутствие стороннего партнера, способного оказать оперативную поддержку и дать экспертные рекомендации в случае инцидента.

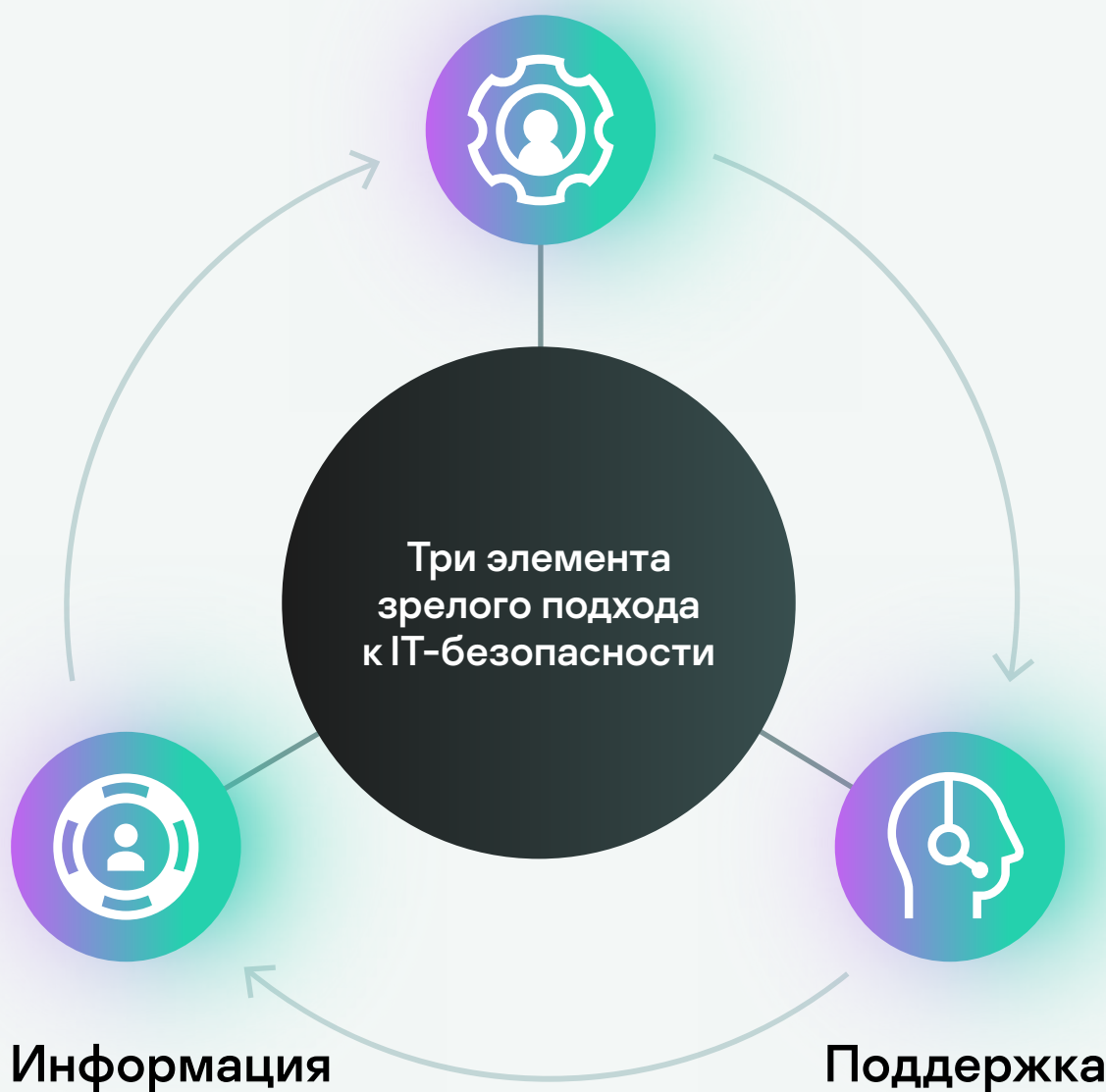
В распоряжении  
вашей команды ИБ  
всё необходимое:  
новейшие  
инструменты,  
точные данные  
и экспертная  
поддержка

## Экспертам – экспертные технологии

**Kaspersky Expert Security** вооружит ваших экспертов современными инструментами для борьбы с продвинутыми кибератаками, предоставит точные и применимые на практике данные об угрозах, а также повысит экспертизу ваших сотрудников. Кроме того, вы также всегда можете рассчитывать на помощь наших экспертов.

### Инструменты

Вооружите ваших специалистов новейшими инструментами для борьбы со сложными угрозами.



Получайте оперативные и достоверные данные об угрозах; развивайте навыки своих экспертов.

Используйте опыт наших экспертов в области анализа защищенности и реагирования на угрозы.

## Инструменты

Снижение рисков информационной безопасности и сокращение потерь от сложных и целевых атак

Повышение продуктивности работы ИБ-служб по выявлению, расследованию и реагированию на сложные киберинциденты

Обеспечение помощи в соответствии требованиям внутренним политикам безопасности и внешних регулирующих органов

Возможность построить экосистему безопасности на основе интегрированных продуктов «Лаборатории Касперского»

## Централизованный сбор и корреляция данных

Разрозненные и неинтегрированные средства защиты малоэффективны против хорошо скоординированных современных атак. «Лаборатория Касперского» предлагает решение **Kaspersky Unified Monitoring and Analysis Platform (KUMA)** — ключевой компонент на пути к реализации единой платформы кибербезопасности. Решение обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, помогает обеспечить соответствие требованиям регулирующих органов и готово встроиться в существующую систему безопасности.

Узнать больше



Kaspersky  
Unified Monitoring  
and Analysis Platform

**Kaspersky Unified Monitoring and Analysis Platform** обеспечивает централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ в реальном времени и своевременное оповещение об инцидентах.

## Мониторинг и расследование инцидентов



Kaspersky  
Threat Intelligence



Kaspersky  
Industrial  
CyberSecurity



Kaspersky  
Security  
для бизнеса



Kaspersky  
Endpoint Detection  
and Response



Kaspersky  
Anti Targeted  
Attack

Единая консоль  
мониторинга и анализа  
инцидентов ИБ



Kaspersky  
Unified Monitoring  
and Analysis  
Platform



Kaspersky  
Threat Lookup



Kaspersky  
CyberTrace



Kaspersky  
Security  
для интернет-шлюзов



Kaspersky  
Secure для почтовых  
серверов



Решения сторонних  
поставщиков



## Инструменты

Сокращение операционных издержек за счет упрощения и автоматизации процессов управления инцидентами

Полная прозрачность корпоративной инфраструктуры и упрощенная организация процесса реагирования на инциденты

Сокращение числа ложноположительных срабатываний и увеличение времени на приоритизацию уведомлений

Сокращение среднего времени обнаружения инцидентов и реагирования на них

# Расширенные возможности обнаружения и реагирования

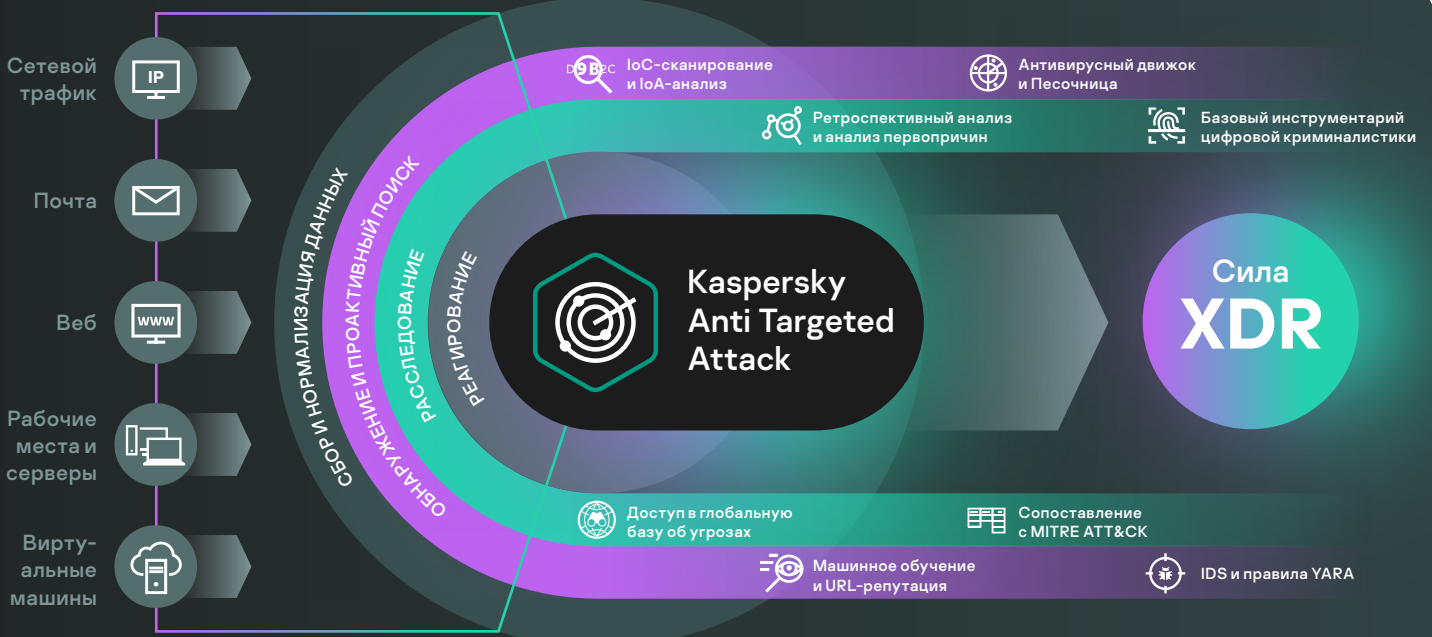
Единая комплексная платформа XDR обеспечивает полную прозрачность корпоративной инфраструктуры и целостность данных, минимизирует количество ложноположительных срабатываний и автоматизирует выполнение рутинных задач по реагированию. Таким образом вы будете надежно защищены от многовекторных атак, в том числе класса APT.

[Узнать больше](#)



## Kaspersky Anti Targeted Attack Platform

Платформа Kaspersky Anti Targeted Attack, объединенная с Kaspersky EDR, предоставляет возможность расширенного обнаружения угроз и реагирования на них. Благодаря интеграции решений и передовым технологиям XDR вы можете контролировать и надежно защищать все точки входа потенциальных угроз: сеть, интернет, электронную почту, конечные устройства и облачные среды.



## Информация

Предоставление контекстных данных на всем протяжении цикла управления инцидентами, что упрощает работу ИБ-специалистов

Повышение окупаемости инвестиций в IT-безопасность за использования данных об угрозах, характерных для вашей отрасли

Простая интеграция с текущими процессами обеспечения безопасности за счет разнообразных форматов предоставления данных

Повышение операционной эффективности системы безопасности, минимизация перебоев в работе и ущерба от инцидентов

## Уникальные аналитические данные

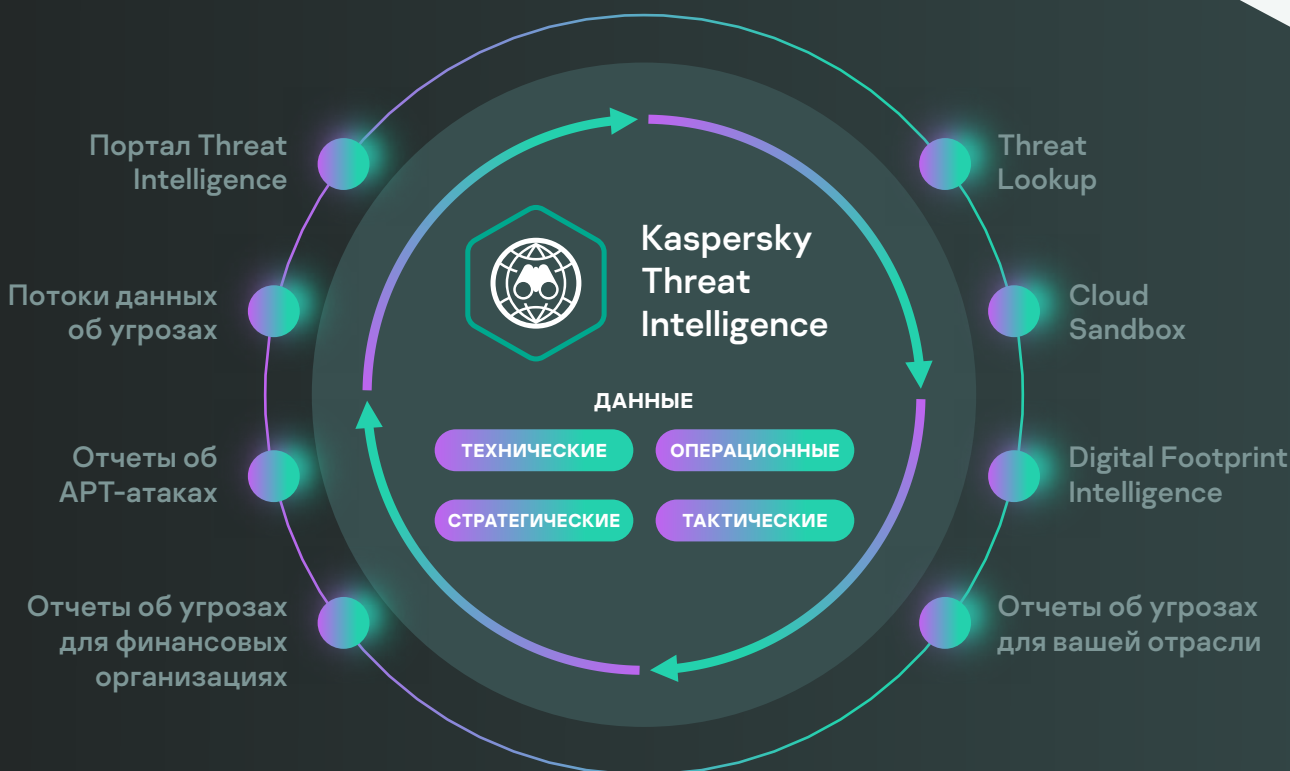
Сотрудникам отдела IT-безопасности следует постоянно повышать свой уровень знаний и оттачивать профессиональные навыки. Постоянное развитие и аналитические данные об угрозах, подготовленные надежным партнером, – залог успешной борьбы с киберугрозами.

Подробнее



Kaspersky  
Threat Intelligence

Интегрируйте оперативные и применимые на практике аналитические данные в вашу систему безопасности. Портал **Kaspersky Threat Intelligence** открывает доступ к актуальным техническим, тактическим, операционным и стратегическим данным об угрозах.



## Информация

Повышение квалификации для быстрого и эффективного уменьшения ущерба от инцидентов

Повышение уровня внутренней экспертизы в области ИБ и возможность анализировать угрозы своими силами

Возможность сохранить в штате и мотивировать сотрудников за счет возможностей профессионального развития

Экономия времени и денег: вам не придется искать новых сотрудников с нужными навыками

## Повышение экспертизы ваших специалистов

Ваши ИБ-специалисты могут повысить экспертизу и получить новые навыки, приняв участие в тренингах **Kaspersky Security Training**. В ходе тренингов участники оттачивают навыки работы с цифровыми уликами, узнают, как анализировать и обнаруживать вредоносное ПО, а также как эффективно реагировать на инциденты.

[Подробнее](#)



**Kaspersky  
Cybersecurity  
Training**

«Лаборатория Касперского» предлагает следующие тренинги для ИБ-специалистов:



Анализ вредоносного ПО



Цифровая криминалистика



Реагирование на инциденты



Использование правил YARA

## Поддержка

Обнаружение попыток компрометации и минимизация ущерба от инцидента еще до того, как он станет явным

Оценка возможностей вашей защиты и выявление слабых мест, требующих внимания

Быстрое восстановление систем и бизнес-процессов

Усиление защиты отраслевых инфраструктур

## Партнёр, которому вы можете доверять

Чтобы определить текущее состояние защищенности ваших систем и эффективно реагировать на сложные инциденты, вам нужен надежный партнер с богатым опытом оказания таких сервисов, обладающий глубокой экспертизой.

## Экспертные сервисы: помощь в анализе защищенности и реагировании на инциденты

Привлекая внешних экспертов, вы сможете просчитать возможные векторы сложных и АРТ-атак и получить практические рекомендации по борьбе с ними. Вам понадобится поддержка надежного партнера, обладающего необходимыми знаниями и опытом, который поможет в экстренной ситуации, оценит уровень защищенности вашей организации, определит потенциальные риски и обеспечит точное реагирование на инциденты.

Подробнее



### Kaspersky Incident Response

Воспользуйтесь преимуществами реагирования на угрозы с помощью экспертов сервиса **Kaspersky Incident Response**, чтобы быстро остановить распространение инцидента и минимизировать его последствия.

Подробнее



### Kaspersky Managed Detection and Response

С **Kaspersky Managed Detection and Response** вы можете положиться на опыт надежного и профессионального партнера. Мы возьмем на себя задачи по управляемому активному поиску угроз, а ваши ИБ-специалисты смогут сосредоточиться на важнейших процессах, требующих их внимания.

Подробнее



### Kaspersky Security Assessment

Воспользуйтесь сервисами анализа защищенности, чтобы проверить готовность вашей системы безопасности к отражению атак и узнать, не стали ли вы уже жертвой скрытой долгосрочной атаки.





## Награды и результаты тестов

«Лаборатория Касперского» активно участвует в независимых тестированиях. Наши технологии и продукты признаны во всем мире и удостоены многочисленных международных наград.

Заслужившее мировое признание сочетание передовых технологий и экспертного опыта



**БОЛЬШЕ ТЕСТОВ  
БОЛЬШЕ НАГРАД  
БОЛЬШЕ ЗАЩИТЫ**

\*[kaspersky.ru/top3](https://kaspersky.ru/top3)



«Лаборатория Касперского» стала лучшим поставщиком EDR-решений в 2020 году по версии Gartner Peer Insights Customers' Choice



**THE RADICATI GROUP, INC.**  
A TECHNOLOGY MARKET RESEARCH FIRM

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете APT Protection Market Quadrant 2020

**GREAT**

GLOBAL RESEARCH  
& ANALYSIS TEAM

В составе «Лаборатории Касперского» действует выделенная команда по исследованию сложных угроз – Global Research and Analysis Team, которая обнаружила множество известных кибератак глобального масштаба

**MITRE | ATT&CK<sup>®</sup>**

Качество обнаружения угроз подтверждено оценкой MITRE ATT&CK

**FORRESTER<sup>®</sup>**

«Лаборатория Касперского» признана лидером по результатам исследования Forrester New Wave: External Threat Intelligence Services (Внешние услуги по анализу угроз), 2021

\*Gartner disclaimer

Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.



Инструменты

Информация

Поддержка

## Коротко о главном

Для успешного противостояния комплексным киберугрозам и эффективной адаптации к новым трудностям в условиях постоянно меняющегося ландшафта угроз вам нужны современные технологии, подкрепленные аналитическими данными об угрозах, опытные специалисты, обладающие необходимыми знаниями, и поддержка внешних экспертов мирового уровня.

В этом случае в вашем распоряжении будет весь комплекс мер противодействия самым сложным APT-угрозам и целевым атакам. В рамках Kaspersky Expert Security мы предлагаем полный арсенал расширенных защитных технологий и сервисов, которые повысят эффективность вашего ИБ-отдела и SOC.

Каковы бы ни были потребности вашего бизнеса сейчас или в будущем, у нас есть решение – **Kaspersky Expert Security.**

[Подробнее](#)

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2021 АО «Лаборатория Касперского».  
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.