Кибер-безопасность крупных IT-инфраструктур

kaspersky

Оглавление

Защита крупных инфраструктур в эпоху цифровой трансформации

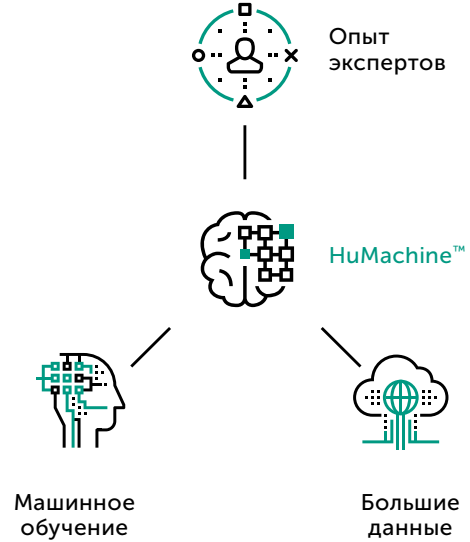
По данным «Лаборатории Касперского», средний ущерб от одного IT-инцидента для компаний крупного бизнеса составляет 14,3 млн рублей. Сегодня уже не возникает вопроса, будет ли атакована ваша компания. Более актуальны другие вопросы: когда и каким образом произойдет атака, как быстро удастся обнаружить угрозу и ликвидировать ее последствия, как защититься от подобных атак в будущем.

В то же время инфраструктура современных компаний становится все более сложной, а облачные сервисы и мобильные устройства размывают традиционное представление о периметре защиты. Кроме того, современные компании все глубже погружаются в цифровую среду, стремясь удовлетворить потребности клиентов и повысить эффективность собственной операционной деятельности. При этом они неизбежно подвергаются новым рискам.

В этих условиях необходимы решения, которые оптимально соответствуют потребностям бизнеса и содержат технологии нового поколения для защиты от передовых угроз.

«Лаборатория Касперского» предлагает обширный портфель решений, продуктов и сервисов, которые обеспечивают как комплексную, так и специализированную защиту инфраструктуры крупного бизнеса, используют накопленную годами экспертизу и новейшие технологии, такие как машинное обучение и обработка больших данных в режиме реального времени.

С решениями «Лаборатории Касперского» вы снизите риск киберугроз и сможете придерживаться намеченных целей в развитии бизнеса.



Контроль и защита рабочих мест

Защита нового поколения от всех видов киберугроз, нацеленных на устройства сотрудников и пользователей

Хакеры и киберпреступники применяют все более изощренные методы атак против IT-инфраструктур крупных компаний. Без надлежащих средств защиты и управления IT-безопасностью предприятия подвергают себя повышенному риску. При этом большинство кибератак производится при помощи рабочих устройств сотрудников. Надежная защита каждого рабочего места может служить основой для эффективной стратегии в области обеспечения безопасности.

Передовые средства обеспечения безопасности рабочих мест:

- Машинное обучение
- Поведенческий анализ
- Адаптивный контроль аномалий
- Защита от шифровальщиков
- Защита от эксплойтов
- Защита от бесфайловых угроз
- Контроль программ, устройств и веб-ресурсов
- Патч-менеджмент
- Встроенное шифрование
- Удаленное развертывание ПО
- Единая консоль управления

Защита как инвестиция в будущее

Средний размер ущерба в результате одного инцидента ИБ для крупных предприятий составляет 14,3 млн рублей. Чтобы избежать подобного ущерба, антивируса уже недостаточно – необходимо комплексное решение, отвечающее за безопасность на нескольких технологических и функциональных уровнях корпоративной IT-инфраструктуры. Истинная защита рабочих мест сочетает в себе различные интеллектуальные методы и технологии для защиты от любых киберугроз на любой платформе. Обезопасив всю корпоративную IT-сеть, вы сможете обеспечить непрерывность бизнеса.

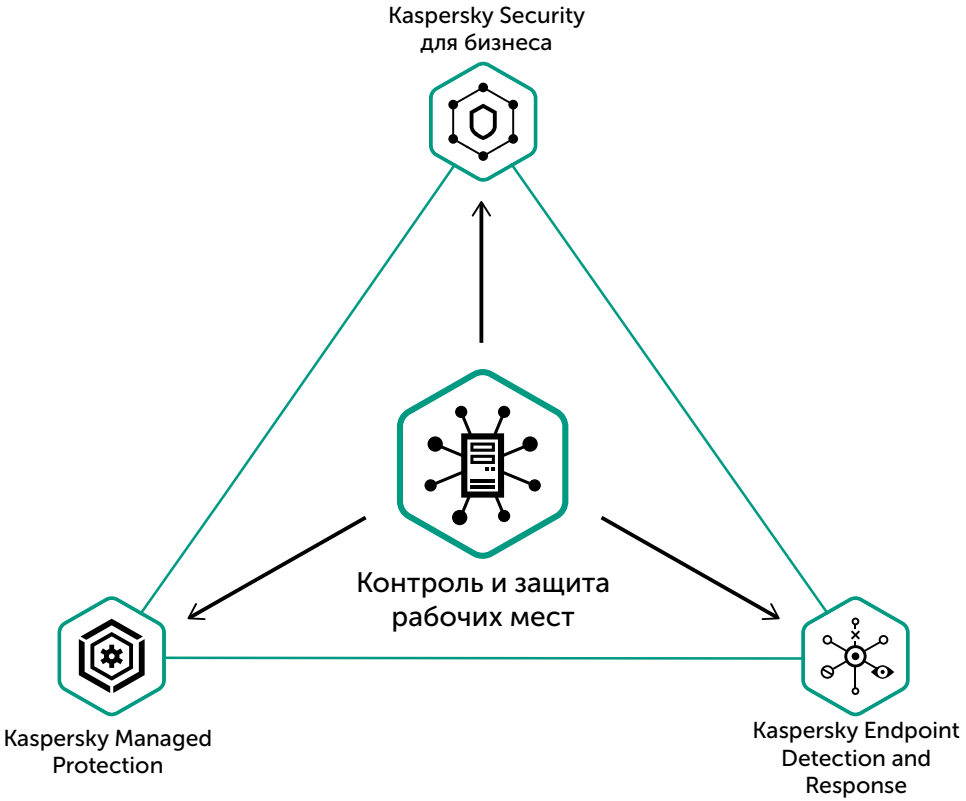
Решение Kaspersky Security для бизнеса обеспечивает комплексную защиту всех рабочих устройств. Оно сочетает сигнатурные и облачные технологии, методы эвристического анализа и инструменты проактивного реагирования для создания многоуровневой системы безопасности рабочих станций и мобильных устройств. Технологии защиты дополняются инструментами контроля, которые помогают управлять приложениями, контролировать или запрещать использование съемных устройств и применять политики безопасного доступа к интернету.

Защита рабочих мест

Технологии защиты рабочих мест представляют собой сочетание традиционных и новейших средств обеспечения безопасности, которые дополнены удобной и функциональной консолью управления. Все решения «Лаборатории Касперского» разработаны на одной технологической базе и тесно интегрированы между собой, что повышает эффективность защиты и снижает стоимость владения.

Платформа защиты рабочих мест включает в себя:

- **Kaspersky Security для бизнеса**
  Гибко масштабируемое решение, удостоенное множества наград. Содержит ряд новейших технологий, в том числе защиту от эксплойтов и вирусов-шифровальщиков.
- **Kaspersky Endpoint Detection and Response**
  Проактивный поиск угроз до того, как они нанесут ущерб, а также средства автоматического реагирования на инциденты.
- **Kaspersky Managed Protection**
  Выделенная служба постоянного анализа событий информационной безопасности.



Защита мобильных устройств

Интегрированные защита и управление для корпоративных мобильных устройств и предотвращение утечки данных

Преимущества мобильных устройств для бизнеса очевидны: они повышают продуктивность работы сотрудников, позволяя получить доступ к информации отовсюду и в любое удобное время. В то же время мобильные устройства, используемые в рабочих целях (BYOD), представляют большую опасность для безопасности компании.

Возможности:

- Защита от вредоносного ПО
- Управление мобильными устройствами (MDM)
- Контроль мобильных приложений
- Обнаружение попыток несанкционированной перепрошивки
- Интеграция с EMM-платформами
- Анти-Bop
- Портал самообслуживания
- Централизованное управление
- решением
- Веб-консоль

Поддерживаемые платформы:

- Android™
- iOS®

Удобство или риск: что перевесит?

Смартфон сегодня есть в кармане практически у каждого человека. Однако это не только удобный инструмент, но и потенциальная угроза для бизнеса. Вредоносное ПО для мобильных устройств, зараженные веб-сайты и фишинговые атаки для мобильных устройств представляют большую опасность. Впрочем, отказываться от мобильных никто не собирается, ведь плюсы использования личных устройств в рабочих целях (BYOD) тоже очевидны – гибкость, простота и оперативность решения рабочих задач. Компании по всему миру ищут баланс между преимуществами и рисками и стремятся проводить в жизнь разумную стратегию обеспечения безопасности мобильных устройств.

Точка входа для сложных атак

Если устройство компактное, это не значит, что и угрозы для него – под стать размеру. Перехват данных, таких как сообщения корпоративной почты, может стать серьезным фактором в конкурентной борьбе и привести к многомиллионным потерям. Кроме того, мобильное устройство рядового сотрудника нередко становится точкой входа для сложных целенаправленных атак. Все это означает, что защищать мобильные устройства необходимо столь же тщательно, как и рабочие станции.

Kaspersky Mobile Security

Приложение Kaspersky Security для мобильных устройств, включающее передовые технологии контроля, защиты и управления, обеспечивает безопасность и надежность использования смартфонов и планшетов в рабочих целях. Решение полностью соответствует потребностям крупных компаний и относится к классу решений Mobile Threat Management (MTM)

Kaspersky Security для мобильных устройств позволяет управлять мобильными устройствами из той же консоли, которая используется для управления другими защитными решениями «Лаборатории Касперского». Просмотр данных на устройствах, создание и администрирование политик, отправка команд на устройства и составление отчетов — все это доступно из единой, простой в использовании консоли управления.

Управление мобильными устройствами (MDM)

В решении доступны групповые политики, позволяющие создавать или активировать правила использования паролей, шифрования, Bluetooth и камеры.

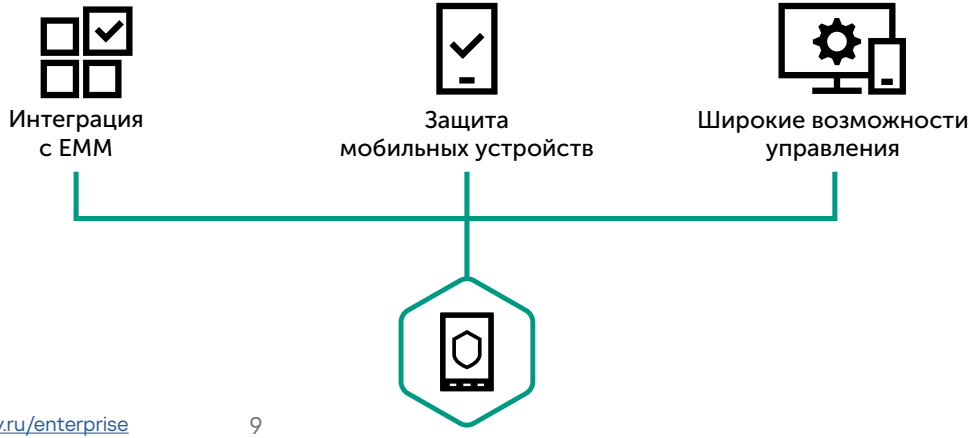
Контроль мобильных приложений

Контроль приложений позволяет разрешить использование только приложений, одобренных администратором, а также получать информацию об установленном ПО и устанавливать приложения.

Интеграция с EMM-платформами

Решение интегрировано с Airwatch® и Citrix XenMobile® и позволяет управлять безопасностью мобильных устройств с помощью вашей EMM-платформы.

Безопасность мобильных устройств



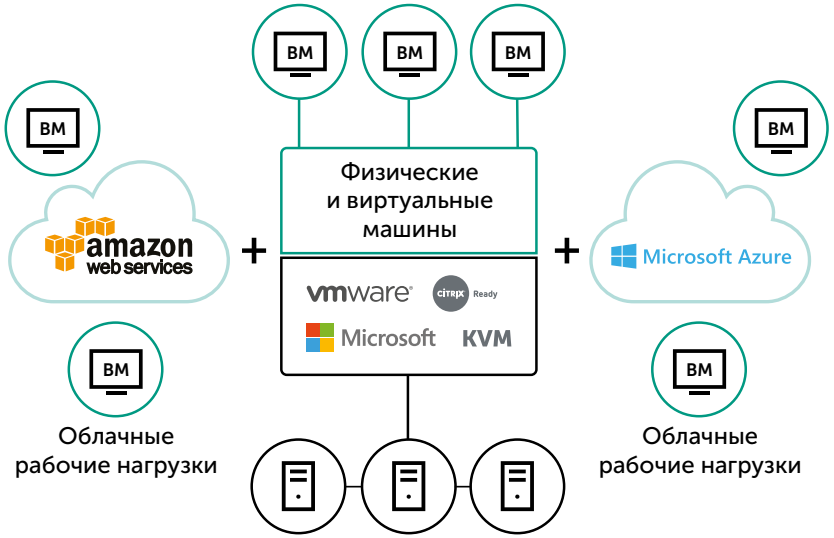
Кибербезопасность виртуальных и облачных сред

Специализированная защита гибридной облачной инфраструктуры

Преимущества решения «Лаборатории Касперского»:

- оптимизация под физические, виртуальные и облачные рабочие нагрузки;
- многоуровневая интегрированная система защиты для любого частного ЦОД;
- гармоничная интеграция гибких и автоматизированных средств безопасности с публичными облаками AWS® и Azure®;
- полный набор инструментов для соблюдения требований по общей ответственности;
- централизованное управление безопасностью всей гибридной облачной среды корпоративного класса.

Решение Kaspersky Security для виртуальных и облачных сред позволяет организовать адаптивную экосистему кибербезопасности с продуманным управлением. Где бы вы ни хранили и обрабатывали критические бизнес-данные – в частном или публичном облаке либо в их сочетании, – сбалансированное сочетание гибких и эффективных средств защиты оградит ваши рабочие нагрузки от самых сложных известных и неизвестных угроз, без ущерба для производительности.



Kaspersky Security для систем хранения данных

Решение обеспечивает надежную, высокоэффективную и масштабируемую защиту ценной и конфиденциальной корпоративной информации, хранящейся в наиболее распространенных СХД.

Основные возможности:

- **Всесторонняя защита в режиме реального времени**

Постоянная проактивная защита сетевых устройств хранения данных (NAS).

- **Оптимизация производительности**

Высокоэффективная проверка с использованием оптимизированной технологии сканирования и возможностью гибкой настройки исключений из проверки.

- **Бесперебойная работа**

Исключительная отказоустойчивость достигается благодаря тесной интеграции и слаженной работе всех компонентов.

Защита нового поколения для физических, виртуальных и облачных сред

- Запатентованные технологии защищают все рабочие нагрузки вне зависимости от их расположения.
- Многоуровневая постоянная защита на базе машинного обучения отвечает за безопасность ваших данных, процессов и приложений

Защита гибридного облака с эффективным использованием ресурсов

- Технологии защиты виртуальных машин на основе легкого агента и без агента позволяют обезопасить программно-определяемые ЦОД без влияния на производительность.
- Интеграция со встроенной системой безопасности публичных и управляемых облачных сред помогает защитить приложения, ОС, пользователей и потоки данных с минимальным расходом ресурсов.
- Объединенное управление физическими и виртуальными ресурсами повышает эффективность администрирования.

Простое управление и полный контроль

- Средства управления безопасностью работают сразу в нескольких облаках.
- Полная видимость, управляемость и комплексная защита от продвинутых угроз доступны в каждой рабочей нагрузке в любой конфигурации.
- Простое развертывание средств безопасности и защита на основе политик по всему гибридному облаку.

Защита от DDoS-атак

Противодействие DDoS-атакам и обеспечение непрерывной работы бизнеса

Одна DDoS-атака может обернуться многочасовыми сбоями и многомиллионными убытками. При этом стоимость проведения таких атак сегодня может составлять всего несколько тысяч рублей.

Преимущества решения «Лаборатории Касперского»:

- Эффективное всестороннее противодействие DDoS-атакам
- Полный охват и успешная работа с атаками большого объема
- Уникальный сенсор для мониторинга трафика в режиме реального времени
- Оперативная круглосуточная защита и поддержка Экспертной группы KDP
- Отказоустойчивая инфраструктура центров очистки расположенных в основных точках обмена интернет-трафика

Борьба с DDoS-атаками на двух фронтах

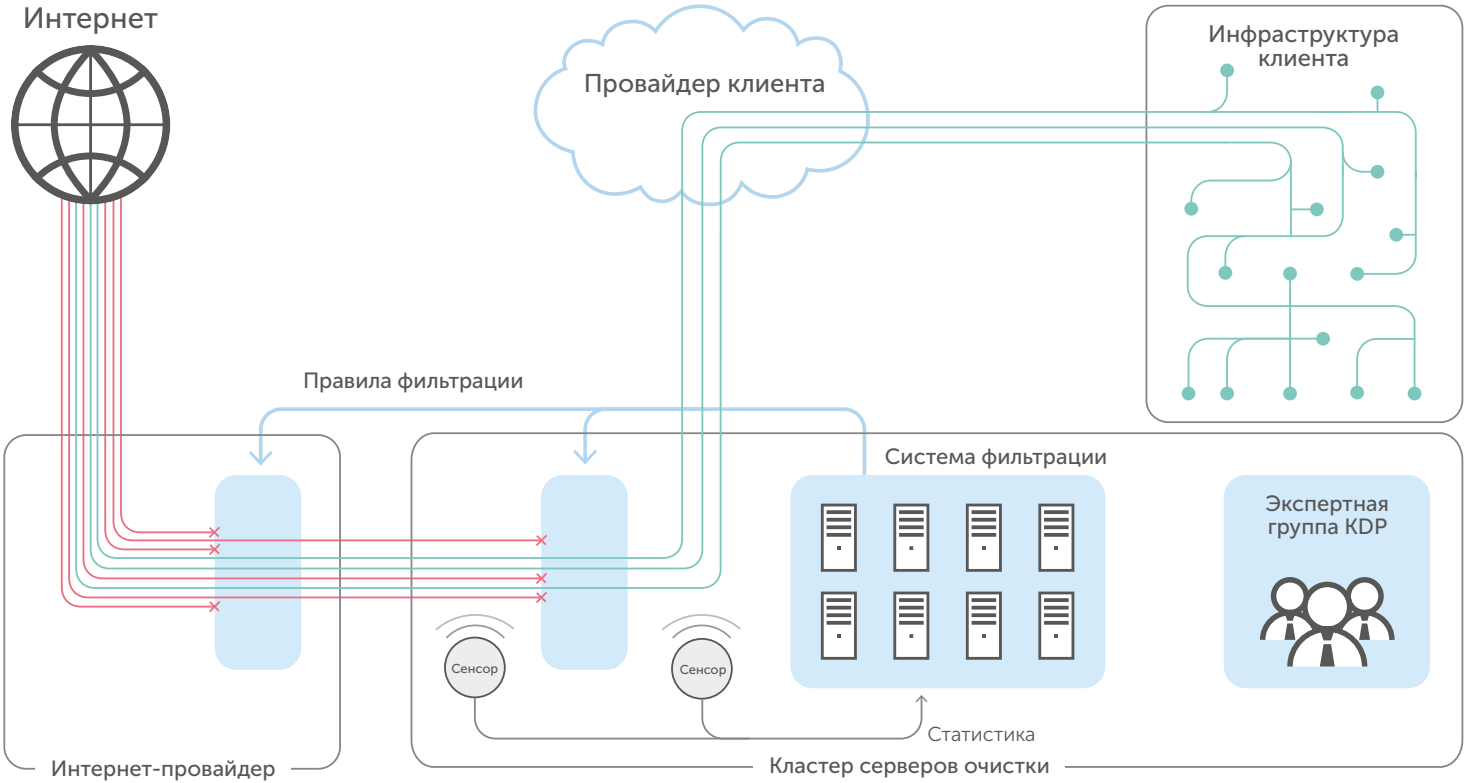
Решение Kaspersky DDoS Protection (KDP) способно распознавать атаки предельно быстро и борется с ними на двух фронтах: через систему мониторинга DDoS Intelligence и с помощью специальной защитной инфраструктуры «Лаборатории Касперского». Кроме того, в «Лаборатории Касперского» работает группа экспертов, которая использует передовые методы, чтобы следить за новейшими DDoS-угрозами и определять угрозы как можно раньше.

Выберите свой вариант противодействия DDoS-атакам

«Лаборатория Касперского» предлагает три версии решения, которые вы можете выбрать в зависимости от ваших целей, ресурсов и сетевой инфраструктуры:

- **KDP Connect** – перенаправление трафика изменением DNS-записи в режиме Always On, доставка очищенного трафика осуществляется через прокси-сервер, GRE-туннели или через выделенную линию.
- **KDP Connect +** – перенаправление трафика средствами протокола BGP в режиме Always On, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.
- **KDP Control** – перенаправление трафика средствами протокола BGP в режиме On Demand, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.

Архитектура Kaspersky DDoS Protection



Защита от целевых атак и сложных угроз

Комплексное решение Kaspersky Threat Management and Defense позволяет эффективно бороться с наиболее сложными и изощренными передовыми угрозами

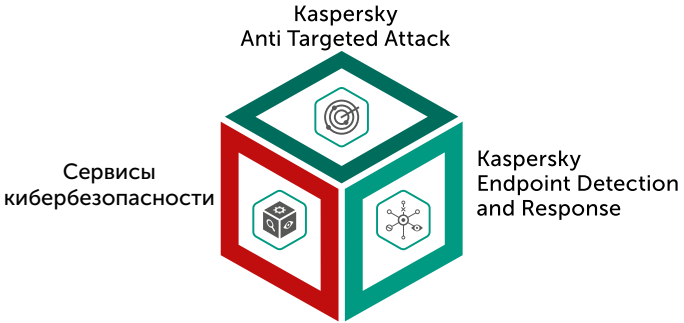
Соответствие требованиям законодательства РФ:

Решения «Лаборатории Касперского» внесены в единый реестр российского ПО, соответствуют требованиям ФСТЭК и ФСБ России, а также учитывают требования российского законодательства:

- Указ Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
- Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В рамках единой стратегии по противодействию передовым угрозам и целевым атакам Kaspersky Threat Management and Defense представляет уникальную комбинацию специализированных защитных средств на базе передовых технологий и широкий спектр экспертных сервисов, способных гибко адаптироваться к потребностям каждой конкретной организации. Решение Kaspersky Threat Management and Defense призвано помочь организациям в соблюдении требований внутренних служб ИБ, внешних регулирующих органов и действующего законодательства в сфере ИБ.

Kaspersky Threat Management and Defense не только автоматизирует процесс сбора данных и упрощает расследование инцидентов, но и предоставляет глобальную аналитику, корреляцию событий на базе машинного обучения и глубокую экспертизу в области анализа киберугроз для противодействия даже самым комплексным атакам на всех этапах их реализации.



Kaspersky Threat Management and Defense – единая платформа по обеспечению быстрого обнаружения угроз, расследования инцидентов, реагирования и восстановления работоспособности инфраструктуры с помощью комплекса взаимосвязанных защитных решений и сервисов:

- **Kaspersky Anti Targeted Attack**
  Специализированная платформа по противодействию комплексным угрозам на всех уровнях IT-инфраструктуры, включающая полнофункциональный набор технологий для обнаружения ранее неизвестных угроз и целевых атак и инструменты сопоставления различных показателей компрометации для выявления атак повышенной сложности.

- **Kaspersky Endpoint Detection and Response**
  Передовое решение по обнаружению инцидентов на рабочих местах и активного реагирования на них за счет организации централизованного управления в корпоративной сети.

- **Сервисы кибербезопасности**
  «Лаборатория Касперского» предлагает различного уровня тренинги для повышения квалификации специалистов в области ИБ, а также предоставляет целый ряд экспертных сервисов, в частности по реагированию на инциденты и активному поиску угроз.

В зависимости от пожеланий заказчика к решению, нормативных требований или особенностей инфрастуруктуры вы можете дополнить решение Kaspersky Threat Management and Defense следующими продуктами:

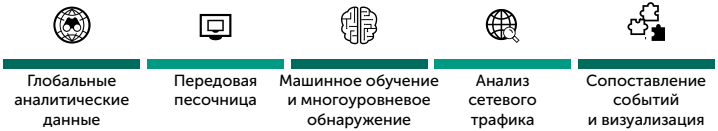
- **Kaspersky Security для бизнеса** – многоуровневая защита рабочих станций и серверов, которая обеспечивает комплексную защиту корпоративной сети и содержит множество передовых технологий, таких как анализ поведения, динамические белые списки, встроенное шифрование файлов или всего диска, поиск и устранение уязвимостей и многие другие.

- **Kaspersky Secure Mail Gateway** – полностью интегрированное решение, объединяющее систему электронной почты и средства ее защиты в составе готового к использованию виртуального устройства безопасности. Продукт обеспечивает самую современную защиту электронной почты от известных и неизвестных угроз, включая спам, фишинг и все виды вредоносных вложений.

- **Kaspersky Private Security Network** – это локальная репутационная база данных, которая соответствует жестким требованиям к системе защиты и обладает всеми преимуществами облачной сети безопасности, но без передачи данных за пределы локальной сети.

Kaspersky Anti Targeted Attack

За счет проверки сетевого трафика в режиме реального времени в сочетании с анализом поведения подозрительных объектов в песочнице и проактивной защитой рабочих мест платформа Kaspersky Anti Targeted Attack дает полное представление о том, что происходит в масштабах даже географически распределенной корпоративной IT-инфраструктуры. Это позволяет обнаруживать угрозы на самых ранних этапах и комплексно реагировать на инциденты любой сложности.



На уровне сети обеспечиваются:

- многоуровневое обнаружение инцидентов и сопоставление событий;
- профилактика атак через электронную почту;
- интеграция с решениями для безопасности сети с целью анализа трафика и обмена вердиктами

Kaspersky Endpoint Detection and Response

Традиционные платформы защиты рабочих мест (Endpoint Protection Platforms) играют важную роль в защите от широкого спектра угроз, включая вредоносное ПО, вирусы-шифровальщики и т. п. В то же время часть угроз могут обходить традиционные средства защиты. Kaspersky Endpoint Detection and Response позволяет обнаруживать подобные инциденты и содержит средства автоматизированного реагирования на угрозы.

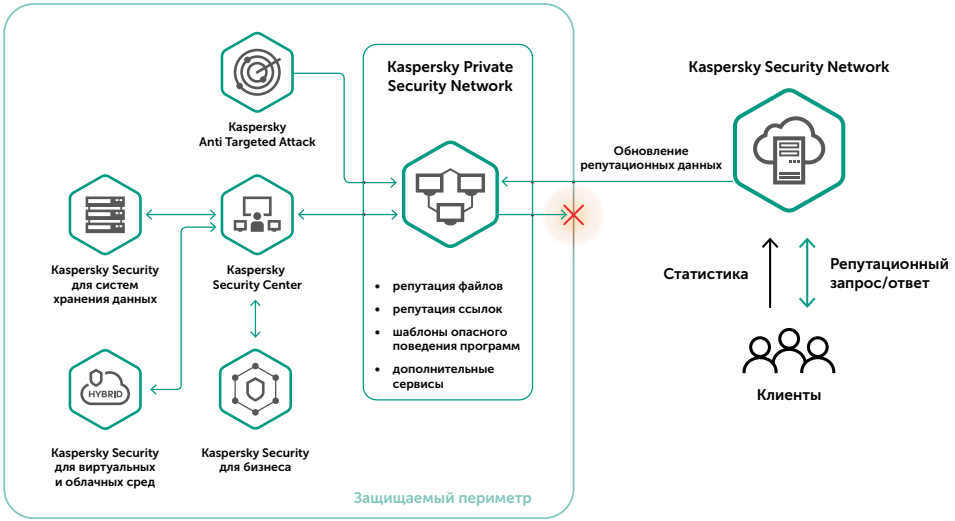
На уровне рабочих мест обеспечиваются:

- обнаружение комплексных угроз;
- проактивный поиск угроз в режиме реального времени и ретроспективный анализ базы данных;
- адаптивное реагирование на угрозы из единого централизованного веб-интерфейса.

Kaspersky Private Security Network

При необходимости соответствия строгим политиками конфиденциальности по обработке критичных данных, «Лаборатория Касперского» предоставляет вариант полностью изолированного репутационной сети, без потери качества обнаружения. Интеграция с Kaspersky Private Security Network, позволяет использовать в работе все преимущества глобального репутационного центра, без передачи данных за пределы контролируемого периметра организации.

Решение Kaspersky Private Security Network можно установить в центре обработки данных организации, и его работу будут полностью контролировать IT-специалисты вашего предприятия. При этом вы не подвергаете риску сохранность конфиденциальных данных и не нарушаете требования IT-безопасности для изолированных сетей.



Сервисы «Лаборатории Касперского»

Широкий спектр сервисов, которые помогают укрепить защиту вашей организации.

Сервисы информирования на угрозы

Сервисы информирования «Лаборатории Касперского» помогают укреплять систему безопасности с помощью потоков данных об угрозах и специализированных отчетов.

- **Потоки данных об угрозах** – постоянно обновляемые потоки данных об угрозах, которые дополняют решение SIEM данными о вредоносных URL-адресах, повышают эффективность решений для защиты сети, расширяют возможности экспертного анализа и помогают в исследовательской работе.

- **Отчеты об APT-угрозах** – новости об обнаружении угроз класса APT не всегда сообщаются сразу, а во многих случаях такая информация вообще не объявляется публично. Наши подробные отчеты позволят вам в числе первых получать эксклюзивную информацию об APT-угрозах.

- **Отчеты об угрозах для финансовых организаций** – отчеты об угрозах, нацеленных на финансовые институты, включая целевые атаки, атаки на инфраструктуру организаций финансового сектора (например, на банкоматы), инструменты, разрабатываемые киберпреступниками для атаки на банки, процессинговые компании, POS-системы.

- **Кастомизированные отчеты** – отчеты, созданные специально для вашей организации. Наши эксперты выстраивают полную картину текущей ситуации с угрозами, выявляют уязвимые места в вашей защите и обнаруживают признаки прошедших, текущих и планируемых атак.

- **Threat Lookup** — онлайн-платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях.

- **Мониторинг ботнет-угроз** – сервис включает подписку на персонализированные уведомления с информацией об обнаруженных ботнетах, атакующих онлайн-ресурсы компании клиента.

- **Мониторинг фишинговых угроз** – сервис активно отслеживает в режиме реального времени появление фишинговых сайтов, угрожающих вашей компании, и своевременно уведомляет о них.

- **Cloud Sandbox** – облачная песочница для изучения подозрительных объектов, в которой используются поведенческий анализ и надежные методы блокировки обхода системы безопасности.

Сервисы анализа защищенности

Экспертные сервисы «Лаборатории Касперского» – это услуги специалистов компании, многие из которых являются признанными во всем мире профессионалами. Их знания и опыт служат опорой нашей репутации мирового лидера в области анализа угроз.

Тестирование на проникновение
Сервис позволит получить более полное представление о проблемных с точки зрения безопасности местах в инфраструктуре, выявить уязвимости, проанализировать возможные последствия атак различного вида и оценить эффективность уже принятых мер защиты, а также получить рекомендации по устранению уязвимостей и повышению безопасности.

Анализ защищенности приложений
Сервис анализа защищенности приложений выявляет уязвимости в приложениях любого типа – от крупных облачных решений, ERP-систем, систем дистанционного банковского обслуживания и других специализированных бизнес-приложений до встроенных программ и мобильных решений на различных платформах.

Анализ защищенности банкоматов и POS-терминалов
Комплексная проверка банкоматов и POS-терминалов на наличие уязвимостей, которые могут использоваться атакующими для несанкционированного снятия наличности, выполнения мошеннических транзакций, сбора данных с карт клиентов или организации DoS-атак.

Анализ защищенности промышленных систем
С помощью сервиса предприятия могут узнать об наиболее уязвимых объектах в инфраструктуре и повысить уровень защиты промышленных систем в соответствии с полученными рекомендациями.

Активный поиск угроз

Киберугрозы могут существовать и действовать внутри корпоративного периметра долгие месяцы, подрывая эффективность работы предприятия и конфиденциальность деловой информации. Именно поэтому возрастает значимость сервисов, которые ищут следы существующей атаки. Сервисы активного поиска угроз «Лаборатории Касперского» помогают обнаружить сложные угрозы при помощи передовых проактивных технологий, передовых технологий и опытных профессионалов.

Сервис обнаружения целевых атак
Сервис «Лаборатории Касперского» по обнаружению целевых атак будет полезен, если вы обеспокоены атаками, направленными на вашу отрасль, заметили подозрительную активность в собственных системах или ваша организация хочет провести плановую профилактическую проверку.

Сервис поможет выявить:
- активные атаки;
- атаки, произошедшие в прошлом;
- скомпрометированные системы.

Кроме того, вы получите рекомендации по устранению последствий атаки и предотвращению подобных атак в будущем.

Kaspersky Managed Protection
Круглосуточная служба анализа событий информационной безопасности. В «Лаборатории Касперского» специально для вашей компании формируется команда экспертов, обладающих обширными навыками и богатым опытом в области анализа угроз. Эти специалисты предоставляют полностью управляемый, индивидуально подобранный сервис непрерывного обнаружения, защиты и анализа, а вы получаете максимальную отдачу от данных, получаемых от установленных в вашей инфраструктуре решений «Лаборатории Касперского».

Сервисы реагирования на инциденты

Остановить атаку до ее проникновения внутрь вашего периметра защиты не всегда возможно, однако снизить возможный ущерб и предотвратить распространение атаки вполне в ваших силах с помощью экспертных сервисов «Лаборатории Касперского».

Сервис реагирования на инциденты
Включает весь цикл расследования инцидента, от сбора улик на месте до выявления дополнительных индикаторов компрометации, подготовки плана борьбы с последствиями и полного устранения угрозы для вашей организации.

Анализ вредоносного ПО
Позволяет получить полное представление о поведении конкретных вредоносных программ, использованных для атаки на вашу организацию, а также о целях, преследуемых злоумышленниками.

Цифровая криминалистика
Эксперты «Лаборатории Касперского» исследуют симптомы инцидента, идентифицируют исполняемый файл вредоносной программы (если он есть) и проводят ее анализ. Клиенту предоставляется подробный отчет с указанием мер, необходимых для устранения последствий инцидента.

Тренинги для IT-специалистов

Тренинги «Лаборатории Касперского» помогут IT- профессионалам получить актуальные знания, расширить свою экспертизу и развить практические навыки в выбранных областях кибербезопасности. Тренинги охватывают широкий спектр тем в области кибербезопасности, а также различных методик и практик, которые могут быть полезны как начинающим специалистам, так и опытным экспертам.

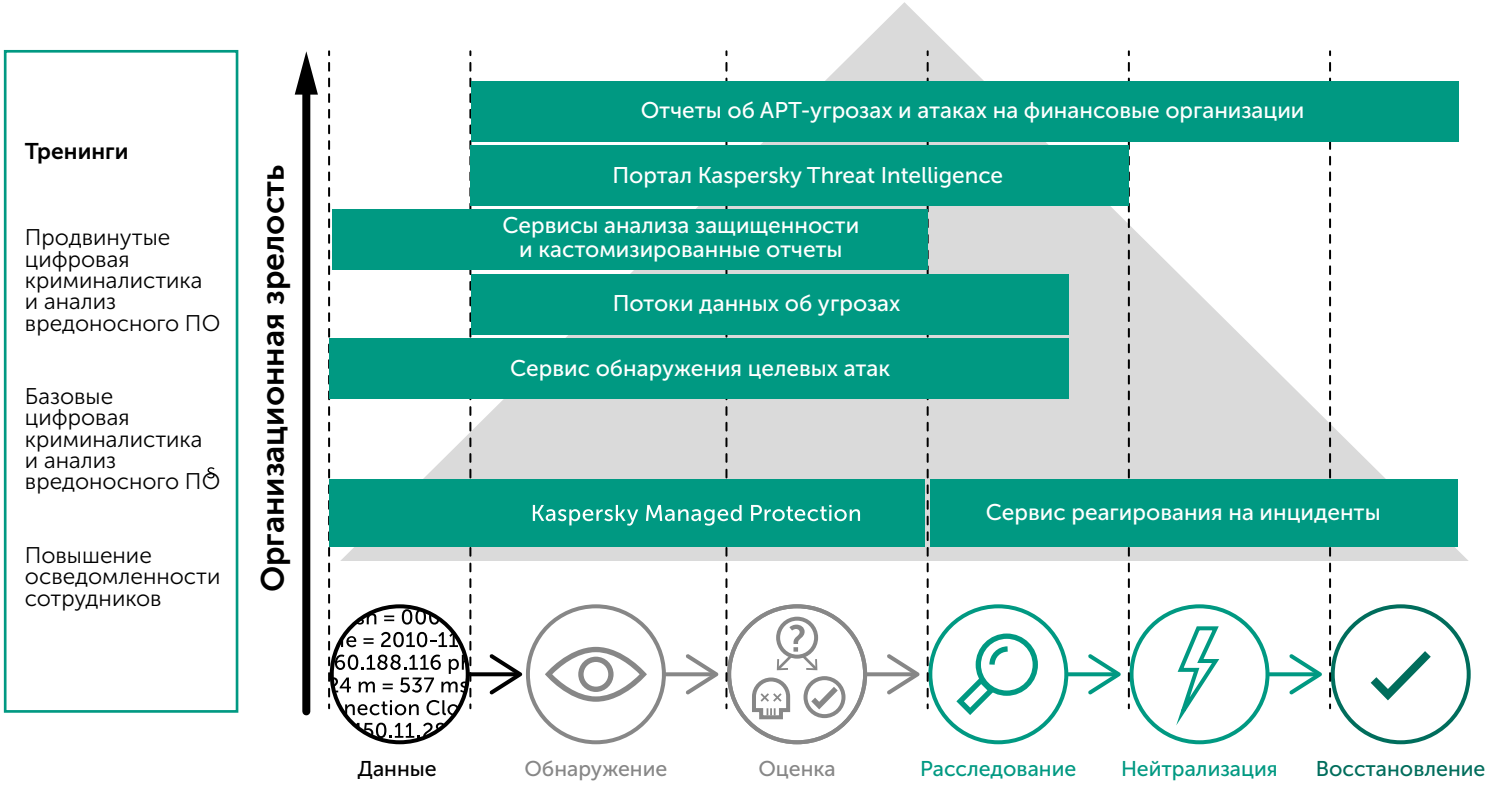
Цифровая криминалистика и продвинутая цифровая криминалистика
Задача тренингов – укрепить знания специалистов во всем, что касается поиска следов киберпреступления и анализа различных типов данных с целью установить источник и временные параметры атаки. После завершения тренинга участники смогут успешно проводить расследование компьютерных инцидентов, что повысит уровень безопасности компании в целом.

Анализ вредоносного ПО и обратная разработка (начальный и экспертный уровни)
Тренинг по обратной разработке поможет специалистам в области реагирования на инциденты успешнее проводить расследование вредоносных атак.

Реагирование на инциденты
Тренинг поможет сотрудникам службы IT-безопасности больше узнать обо всех стадиях расследования инцидентов и даст все необходимые сведения для успешного самостоятельного устранения последствий инцидента.

Обнаружение угроз с помощью YARA
Тренинг поможет узнать, как правильно писать, эффективно тестировать и улучшать правила YARA таким образом, чтобы с помощью них можно было успешно обнаруживать атаки.

Сервисы кибербезопасности «Лаборатории Касперского»



Программы повышения осведомленности

Эффективный метод укрепления корпоративной культуры интернет-безопасности

Более 80% всех киберинцидентов связаны с человеческим фактором. Предприятия тратят огромные средства на восстановление ресурсов после инцидентов безопасности, вызванных действиями сотрудников. Однако традиционные программы обучения, призванные предотвращать такие нарушения, недостаточно эффективны. Они информируют, но не мотивируют. Программы повышения осведомленности «Лаборатории Касперского» не только дают знания, но и формируют правильное поведение.

Преимущества программы

- Наши курсы не только дают знания, но и закладывают основы безопасного поведения: при обучении используются игровой подход, практические занятия, имитация атак и т. д. Это позволяет формировать устойчивые привычки и укреплять кибербезопасность в долгосрочной перспективе.
- Для разных категорий сотрудников формируются разные навыки. Высшее руководство, линейные руководители/менеджеры среднего звена, IT-специалисты и рядовые специалисты — все эти группы сотрудников обучаются разным навыкам с учетом их должностных обязанностей.
- Большинство курсов проходят в онлайн-формате, поэтому формат позволяет и отделу ИБ, и отделу кадров легко отслеживать успеваемость пользователей и контролировать ход обучения.
- В основе курсов – богатый опыт «Лаборатории Касперского» в области кибербезопасности и разработки защитных решений.

Программы повышения осведомленности

Kaspersky Interactive Protection Simulation

Игра Kaspersky Interactive Protection Simulation (KIPS) предназначена для руководителей компаний, корпоративных экспертов по кибербезопасности и сотрудников IT-отделов. Цель тренинга: повысить осведомленность о рисках и проблемах безопасности, связанных с использованием современных компьютерных систем, а также продемонстрировать влияние киберугроз на результаты бизнеса.

Доступные сценарии:

- Корпорация
- Банк
- Электронное правительство
- Нефтяная компания
- Электростанция
- Станция водоочистки
- Транспорт

Каждый сценарий построен вокруг наиболее актуальных для данной отрасли векторов угроз. Это позволяет выявлять и анализировать типичные ошибки в отношении стратегии кибербезопасности и реагирования на инциденты.

Игровые тренинги Kaspersky Cybersafety Management Games

Kaspersky CyberSafety Games – это интерактивный мастер-класс, который включает компьютерные занятия и уроки под руководством инструктора. Тренинг показывает линейным руководителям всю важность кибербезопасности на их уровне ответственности. Помимо создания необходимых знаний и компетенций, игровой курс помогает выработать правильное отношение к поддержанию безопасной рабочей среды во всем подразделении.

Обучение IT-специалистов навыкам поддержания кибербезопасности

Стандартные программы повышения осведомленности не затрагивают IT-профессионалов, службу IT-поддержки и других технических сотрудников. «Лаборатория Касперского» представляет программу обучения, предназначенную специально для IT-специалистов, которая учитывает их высокий уровень технической осведомленности.

Kaspersky Automated Security Awareness Platform

Онлайн-платформа обучения навыкам Kaspersky Automated Security Awareness Platform – ключевой компонент программы повышения осведомленности. Она помогает пользователям освоить разные сценарии и ситуации, получить больше знаний и понять, как определять и реагировать на распространенные киберугрозы. Онлайн-обучение позволяет практиковаться и учиться на интерактивном портале.

Преимущества:

- Увлекательные обучающие модули
- Точная оценка знаний
- Имитации реальных атак
- Регулярные отчеты и анализ

Защита критической инфраструктуры

Стратегический подход к кибербезопасности промышленных сред

Число вредоносных атак на промышленные системы, в том числе на автоматизированные системы управления технологическими процессами (АСУ ТП) в последнее время значительно возросло. Одного зараженного USB-накопителя может быть достаточно, чтобы вредоносное ПО распространилось по всей индустриальной сети.

Kaspersky Industrial Cybersecurity

- Защищает производственные предприятия от киберугроз
- Обеспечивает безопасность промышленных сред и непрерывность производственных процессов
- Минимизирует время простоев и задержки технологических процессов

Системы АСУ ТП требуют совершенно иного подхода к IT-безопасности по сравнению с классической офисной IT-инфраструктурой. В корпоративных средах основное внимание уделяется сохранности конфиденциальных данных, а бесперебойная работа не настолько важна, как для систем управления производственными процессами, где цена минуты простоя, как и любой другой ошибки, очень велика. Поэтому в обеспечении безопасности производственных процессов действует противоположный подход, при котором основной задачей является поддержание их непрерывности и оперативное устранение любых сбоев.

Еще одно отличие заключается в используемых технологиях. Большинство корпоративных сетей строятся на базе «классических» ОС и программ, в то время как промышленные системы, как правило, отличаются исключительной сложностью и задействуют узкоспециализированные технологии, что требует от системы безопасности дополнительной гибкости.

При разработке решения для защиты промышленных предприятий «Лаборатория Касперского» сделала акцент на обеспечении непрерывности технологических процессов. В основе подхода лежат многолетняя экспертиза в области кибербезо-пасности, глубокое понимание природы уязвимостей информационных систем и тесное сотрудничество с международными и российскими регуляторами в области требований к защите.

Решение Kaspersky Industrial CyberSecurity создано специально для защиты сложных промышленных сред, отличается высокой гибкостью и настраивается в соответствии с потребностями вашего предприятия.

Kaspersky Industrial CyberSecurity

ПРОДУКТЫ

Защита конечных узлов

KICS for Nodes

Мониторинг сетей и обнаружение вторжений

KICS for Networks

Централизованное управление

Kaspersky Security Center

СЕРВИСЫ

Тренинги

Kaspersky Security Awareness

Kaspersky Security Training

Экспертные сервисы

Kaspersky Security Assessment

Kaspersky Incident Response

Kaspersky Threat Intelligence

Защита мобильного и онлайн-банкинга

Снижение риска мошенничества при совершении финансовых операций

Клиенты все реже посещают отделения банков и предпочитают совершать банковские операции, используя компьютер и телефон. Разумеется, эту тенденцию заметили многие финансовые организации — они активно запускают мобильные приложения и разрабатывают онлайн-сервисы. Это привлекает не только новую аудиторию, но и киберпреступников.

Атаки на счета и транзакции

Для похищения денег через интернет-банки и сайты финансовых услуг киберпреступники применяют разнообразные схемы.

- К основным угрозам относятся:кража учетной записи – атака, при которой злоумышленник получает доступ к аутентификационным данным пользователя и использует их для осуществления нелегитимных операций;
- кража персональных данных пользователя — на основе этих данных создаются ложные учетные записи от лица пользователя (для мошенничества или нелегального вывода денег);
- вмешательство в транзакции — изменение параметров транзакции или создание новой транзакции от имени пользователя.

Kaspersky Fraud Prevention

Kaspersky Fraud Prevention не просто устраняет последствия мошеннического инцидента, но дает организациям возможность принять превентивные меры, чтобы не позволить злоумышленникам добиться своей цели. Платформа активно блокирует попытки киберпреступников похитить данные пользователей, устраняя угрозу мошенничества до того, как она получит реальное воплощение. Консоль решения также позволяет сотрудникам банка, отвечающим за борьбу с мошенничеством, собрать точные сведения о каждом инциденте, в том числе учетные данные, использованные для доступа к счету.

Защита в режиме реального времени

Kaspersky Fraud Prevention относится к системам следующего поколения, которые позволяют в режиме реального времени анализировать поведение, устройства и окружение пользователя, а также с помощью машинного обучения выявлять продвинутые схемы мошенничества и отмывания денег. Кроме того, Kaspersky Fraud Prevention помогает эффективно защищать мобильные устройства пользователей от попыток онлайн-мошенничества.

Advanced Authentification

Решение, созданное для повышения удобства пользователей, снижения затрат на двухфакторную аутентификацию и оперативного обнаружения подозрительной активности. Применение Advanced Authentication способствует росту бизнеса и повышению уровня безопасности предоставляемых услуг.

Аутентификация на основе рисков

Технологии машинного обучения и непрерывный анализ сотен параметров в режиме реального времени позволяют динамически оценивать риски, чтобы вы могли принять быстрое и точное решение: позволить ли пользователю войти, провести дополнительную верификацию или ограничить его доступ.

Непрерывная аутентификация

Решение анализирует поведенческие и биометрические данные, репутацию устройства и другую важную неперсонифицированную информацию. Если система обнаруживает какие-либо признаки аномального или подозрительного поведения, она автоматически отправляет соответствующий сигнал в систему аутентификации, позволяя ограничить мошенническую активность еще до совершения транзакции.

Обнаружение кражи учетной записи

Kaspersky Fraud Prevention на этапе входа в систему выявляет новые, неиспользованные ранее устройства, через которые осуществляется вход в личный кабинет. Кроме того, анализ поведенческих и биометрических данных в режиме реального времени определяет отклонения от «типичного» пользовательского поведения, выявляя использование устройства или учетной записей мошенником.

Automated Fraud Analytics

Позволяет обнаруживать возможную мошенническую активность, когда она еще не началась, и предоставляет все данные и аналитику, необходимые для принятия точных и своевременных решений при выявлении особо сложных случаев.

Автоматическое построение и сопоставление связей

Показывает невидимые и неочевидные связи между устройствами, организациями и окружениями. Работает в кросс-канальных и кросс-организационных средах, выявляя корреляцию между типичными профилями, используемыми устройствами, шаблонами поведения и другими параметрами пользовательских сессий. Доступ к этим данным дает вам ключ к раскрытию сложных мошеннических схем.

Поведенческий анализ на основе глубинного обучения

Снижает необходимость разработки функционала и упрощает процесс адаптации при выявлении новых профилей поведения как легитимных пользователей, так и злоумышленников. Автоматически обнаруживает необычное и подозрительное поведение на этапе входа в систему и на протяжении всей сессии, не пропуская даже самые незначительные отклонения от нормы.

Гибкая настройка правил

Позволяет вам контролировать уровень и объем создания инцидентов. Готовые к использованию подробные инциденты могут быть настроены с учетом мошеннических схем, актуальных для вашего бизнеса.

Защита банкоматов и POS-систем

Специализированная защита для встраиваемых систем

Банкоматы и POS-системы привлекают киберпреступников тем, что они непосредственно связаны с финансовыми транзакциями, выдачей наличных денег и считыванием данных банковских карт. Защитить встроенные системы особенно трудно: обычно они распределены географически, сложны в управлении и редко обновляются. Таким устройствам требуется направленная защита высочайшего уровня.

Kaspersky Embedded Systems Security

«Лаборатория Касперского» создала решение Kaspersky Embedded Systems Security для защиты банкоматов, кассовых систем и киосков самообслуживания. Оно создано с учетом актуальных угроз, функционала устройств, особенностей операционных систем, соединений и архитектуры встраиваемых систем.

Низкие требования к аппаратным ресурсам

Решение «Лаборатории Касперского» рассчитано на полноценную работу на низкопроизводительных аппаратных платформах, которыми оборудованы большинство банкоматов и POS-систем. Системные требования к оборудованию минимальны. При использовании режима проверки по требованию решение обращается к аппаратным ресурсам только во время проверок на вирусы.

Поддержка Windows XP

Около 90% банкоматов по-прежнему используют ОС семейства Windows XP, поддержка которого прекращена производителем. Решение Kaspersky Embedded Systems Security оптимизировано для полнофункциональной работы на платформе Windows XP, так же как и на ОС Windows 7, Windows 2009 и Windows 10 IoT.

Соответствие требованиям PCI DSS

Согласно требованиям PCI DSS, все системы, которые работают с банковскими картами, должны быть снабжены регулярно обновляемым антивирусом. Kaspersky Embedded Systems Security полностью соответствует этим требованиям.

Контроль целостности файлов*

Контроль целостности файлов отслеживает действия с выбранными файлами и папками. Также можно отслеживать изменения в файлах, произошедшие тогда, когда мониторинг был прерван.

Аудит записей журнала*

Решение отслеживает целостность защищаемой среды, основываясь на записях в журнале событий Windows.

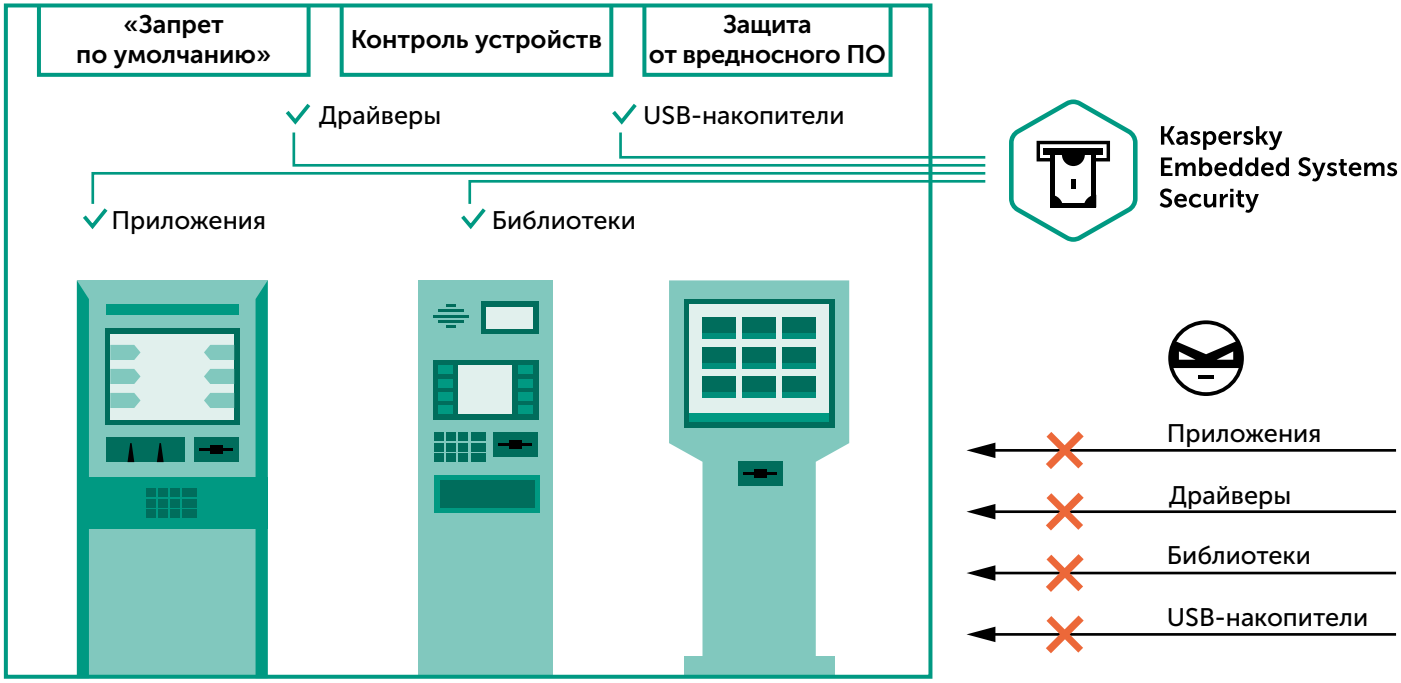
*Данные функции доступны в версии KESS Compliance Edition.

Сценарий «Запрет по умолчанию»

При использовании этого сценария в системе исполняются только те файлы, драйверы и библиотеки, которые явно разрешены администратором. Это позволяет защититься от комплексных атак.

Контроль устройств

Функция контроля устройств позволяет контролировать доступ к системе USB-носителей — один из основных путей проникновения во встроенные системы.



Расширенная техническая поддержка

Реакция на критически важные события в режиме 24x7 и прямой доступ к техническим специалистам

Премиальные программы поддержки идеально подходят крупным компаниям, для которых исключительно важна непрерывность бизнес-процессов. Решение вашей проблемы становится приоритетной задачей для экспертов «Лаборатории Касперского».

Преимущества MSA Enterprise:

- **Быстрое реагирование.** Специальная группа дежурит в режиме 24/7, отвечая за максимально быстрое решение ваших проблем.
- **Минимум риска.** Меры безопасности, адаптированные к вашей системе (включая приоритетные хотфиксы и персонализированные исправления), обеспечивают полную защиту.
- **Знание особенностей вашей инфраструктуры.** Каждому клиенту MSA Enterprise выделяется персональный технический менеджер.

Результат таких энергичных действий и экспертного подхода — снижение числа простоев, более быстрое восстановление систем и экономия внутренних ресурсов, необходимых для устранения неполадок.

Программы премиальной поддержки

	MSA Business	MSA Enterprise
	Решение для компаний, которым требуется реакция на критически важные события в режиме 24x7 и прямой доступ к техническим специалистам	Решение для компаний со сложной инфраструктурой, которым требуется персонализированная и проактивная защита
24x7x365	✓	✓
Выделенная телефонная линия	✓	✓
Время реакции на критические инциденты	4 часа	30 минут
Персональный технический менеджер		✓
Регулярные отчеты о статусе решения проблемы		✓

Профессиональные услуги

Получите максимум преимуществ от продуктов «Лаборатории Касперского»

Компании, которые заботятся о кибербезопасности, вкладывают серьезные средства в укрепление защиты. Эксперты «Лаборатории Касперского» помогут получить максимальную отдачу от этих инвестиций. Специалисты по профессиональным услугам помогут вам быстрее развернуть решения «Лаборатории Касперского», а также оптимизировать и настроить их так, как нужно именно вашей компании.

Помощь экспертов

В рамках профессиональных услуг эксперты «Лаборатории Касперского», помогут научиться использовать продукты наиболее эффективно. Сложность внедрения и затраты на него минимизированы, а процесс знакомства с продуктом значительно сокращен. Лучшие практические методики, разработанные на основе богатого опыта работы с клиентами, многократно ускоряют развертывание решений.

Развертывание

Эксперты «Лаборатории Касперского» разъяснят возможности защитных решений и подскажут, как пользоваться ими с учетом оборудования и потребностей компании. Корректное развертывание в перспективе избавит от многих проблем с избыточной нагрузкой на сети.

Обновление

В рамках услуги Обновления эксперты оказывают дополнительную техническую помощь при развертывании новых версий продуктов «Лаборатории Касперского» для того, чтобы обновление прошло гладко и никак не повлияло на работу компании.

Проверка состояния системы защиты

После полного аудита настроек продуктов и сетевой среды (дистанционного или на территории клиента) специалисты создают подробный отчет с практическими рекомендациями: например, как повысить эффективность защиты и системы ее управления. Таким образом, процесс развертывания решения с самого начала оптимизируется для конкретной инфраструктуры и систем клиента.

Настройка

После комплексной оценки конкретных требований, политик и инфраструктуры клиента эксперты «Лаборатории Касперского» предоставляют набор рекомендаций, в том числе наиболее эффективные конфигурации и настройки политик безопасности.

Консалтинг

Консультанты «Лаборатории Касперского» помогут укрепить систему безопасности каждого клиента индивидуально, с учетом его потребностей. В рамках сервиса клиенты получают рекомендации и советы, проходят целенаправленное обучение и специализированные тренинги.

Защита отдельных узлов сети

Специализированные решения для обеспечения безопасности отдельных компонентов сети

Все устройства в составе корпоративной сети нуждаются в надежной специализированной защите. Поэтому, помимо решения для контроля и защиты рабочих мест, «Лаборатория Касперского» разработала продукты для обеспечения безопасности отдельных узлов сети. Они могут быть установлены в дополнение к продуктам Kaspersky Security для бизнеса или как отдельное решение.

Защита файловых серверов

Kaspersky Security для файловых серверов — это эффективное, надежное и масштабируемое решение для защиты файловых хранилищ с общим доступом, не оказывающее заметного влияния на производительность системы. Решение обеспечивает защиту от вредоносного ПО для серверов на базе Linux и Windows.

Защита интернет-шлюзов

Kaspersky Security для интернет-шлюзов проверяет трафик HTTP, HTTPS и FTP в режиме реального времени и обеспечивает всестороннюю защиту интернет-шлюзов от известных и вновь возникающих угроз.

Защита почтовых серверов

Kaspersky Security для почтовых серверов обеспечивает защиту почтового трафика от спама, фишинговых ссылок и вредоносного ПО. Решение поддерживает популярные почтовые платформы Microsoft Exchange и Linux® Mail Server.

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

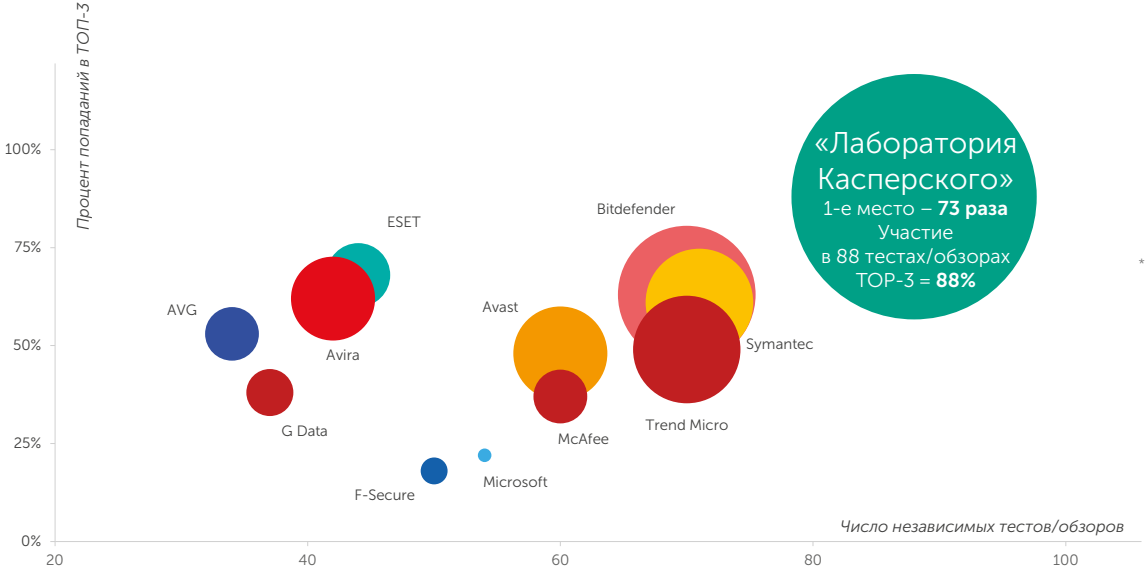
«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз. Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Более подробная информация доступна на www.kaspersky.ru.

Больше тестов. Больше наград. Больше защиты*

В 2018 году продукты «Лаборатории Касперского» приняли участие в 88 независимых тестах и обзорах. В 73 случаях они заняли первое место и 77 раз вошли в тройку лучших (ТОП-3).



БОЛЬШЕ ТЕСТОВ
БОЛЬШЕ НАГРАД
БОЛЬШЕ ЗАЩИТЫ

* Примечания:

- По результатам независимых тестов корпоративных, потребительских и мобильных продуктов за 2018 год.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AV-Comparatives, AV-Test, SE Labs, MRG Effitas, Virus Bulletin, ICSA Labs, NSS Labs, PCSL.
- Тестировались все доступные технологии защиты против известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест.
- Подробнее: www.kaspersky.ru/top3

kaspersky

www.kaspersky.ru