



## Kaspersky Security для бизнеса

# Защита от киберугроз

Если механизм предотвращения угроз слаб, то и любое решение безопасности на его основе тоже будет неэффективным. Патч-менеджмент, шифрование, инструменты контроля – эти и другие технологии обеспечивают важную дополнительную защиту, но не могут компенсировать недостатки базовой защиты от угроз.

Защита от угроз находится в центре каждого решения «Лаборатории Касперского». Наш многоуровневый гибкий подход включает множество слоев, которые противодействуют киберугрозам в разных их проявлениях и на разных уровнях. В продуктах «Лаборатории Касперского» для защиты рабочих мест реализован целый арсенал превентивных технологий нового поколения, которые обнаруживают, минимизируют и нейтрализуют самые изощрённые и актуальные угрозы.

## Экспертные знания и исследование угроз

Защита нового поколения строится на базе нашей концепции HuMachine™, которая объединяет в себе технологии машинного обучения, экспертные знания и глобальную аналитику угроз. Эксперты «Лаборатории Касперского» обнаружили больше АРТ-угроз мирового масштаба, чем любой другой производитель решений информационной безопасности. Мы твердо намерены и далее вкладывать ресурсы изучение угроз, что подтверждает как количество наших исследовательских команд, так и их признание мировым сообществом.

## Многоуровневая защита на основе передовых технологий

Многоуровневая защита достигается благодаря комбинированному использованию технологий, разработанных на базе алгоритмов машинного обучения. Современные средства защиты рабочих станций и усиление защиты систем (включая поддержку белых списков и контроль программ), поведенческий анализ для обнаружения атак, автоматизированное устранение последствий атаки, защита от эксплойтов и программ-вымогателей – всё это входит в наши решения для защиты конечных устройств. Также предоставляется защита от скриптов PowerShell и бесфайловых атак.

## Kaspersky EDR – надёжный инструмент поиска и обнаружения угроз

Интеграция с Kaspersky Endpoint Detection and Response обеспечивает автоматическое реагирование на инциденты безопасности. Этот комплексный подход к применению EDR повышает прозрачность во всех сегментах IT-инфраструктуры, позволяя центрам обеспечения безопасности принимать информированные решения и выбирать лучшие стратегии для нейтрализации как низкоприоритетного вредоносного ПО, так и самых продвинутых угроз.

## Широкие возможности управления для крупных компаний

Возможность управлять сотнями и тысячами рабочих станций из единой консоли позволяет гибко контролировать всю ИТ-инфраструктуру и видеть полную картину её безопасности. Для корпоративных систем крупного бизнеса поддерживаются такие возможности, как автоматизированное развёртывание ПО, автоматическое создание отчетов, а также поддержка иерархических и изолированных сред.

# Дополнительные функции

## Базовая защита от угроз

### Защита от файловых угроз

Этот обязательный компонент обладает большим набором технологий для защиты от файловых угроз. Сюда также входит сканирование подсистемы Windows Subsystem for Linux (WSL).

### Защита от почтовых угроз

Чаще всего вредоносное ПО проникает в корпоративную сеть именно через электронную почту. Компонент «Защита от почтовых угроз» проверяет входящие и исходящие письма на наличие опасных объектов.

### Защита от веб-угроз

Этот компонент защищает данные, которые поступают на компьютер и отправляются с него, устанавливает принадлежность URL-адресов к вредоносным или фишинговым веб-адресам, а также проверяет HTTPS-трафик, чтобы своевременно пресечь действия агентов ботнетов, дропперов, вирусов-вымогателей и т. д.

### Защита от сетевых угроз

Этот компонент отслеживает во входящем трафике активность, характерную для сетевых атак. Защита от MAC-спуфинга помогает идентифицировать и запрещать подмену адресов, которая делается для компрометации рабочих станций и перехвата трафика, адресованного другим устройствам сети.

### Сетевой экран

Этот компонент фильтрует сетевые пакеты, потоки данных и сетевые соединения, тем самым ограничивая сетевую активность устройства.

### Защита от атак BadUSB

Компонент «Защита от атак BadUSB» разрешает использовать авторизованную клавиатуру и запрещает неавторизованную, которую имитирует заражённое USB-устройство.

### Технология AMSI

AMSI (Anti-Malware Scan Interface) позволяет решению «Лаборатории Касперского» проверять отправленные сторонними программами объекты. Результаты проверки передаются этой программе, которая в свою очередь может заблокировать или удалить объект.

## Продвинутая защита от угроз

### Kaspersky Security Network (KSN)

Облачная репутационная база данных об угрозах собирает и анализирует данные о безопасности того или иного объекта, которые добровольно предоставляются миллионами пользователей по всему миру. KSN обнаруживает вредоносное ПО и максимально быстро реагирует на новые угрозы.

### Анализ поведения

Данный компонент использует технологии машинного обучения для обнаружения и извлечения шаблонов опасного поведения, чтобы эффективно защитить систему от вирусов-вымогателей. Анализ поведения может обнаружить и остановить вредоносное шифрование локального файла и удалённое шифрование общих папок через сеть.

### Защита от эксплойтов

Защита от эксплойтов отслеживает вредоносное ПО, которое эксплуатирует уязвимости наиболее распространённых программ. Сначала она обнаруживает подозрительные модели поведения, затем немедленно останавливает эксплуатацию и предотвращает выполнение уже загруженного вредоносного кода.

### Система предотвращения вторжений на уровне хоста (HIPS)

На основе данных KSN образуются четыре стандартные группы доверенных программ, а HIPS распределяет программы по этим группам. Самые доверенные из них заносятся в белый список и запускаются без ограничений. Остальные имеют ограниченные привилегии и лимитированный доступ к критическим сетевым ресурсам.

### Откат вредоносных действий

Этот компонент собирает данные о подозрительной активности, что позволяет выполнить откат действий, которые были произведены вредоносными программами.

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

© 2020 АО «Лаборатория Касперского».  
Все права защищены. Зарегистрированные  
товарные знаки и знаки обслуживания  
являются собственностью  
их правообладателей.