



▶ **ПРОДУКТЫ  
ДЛЯ БИЗНЕСА 2014**

Контроль и защита из единого центра

**KASPERSKY** 

## ▶ О КОМПАНИИ

«Лаборатория Касперского» входит в число крупнейших мировых производителей решений для обеспечения информационной безопасности. Мы предоставляем организациям решения для обеспечения максимального уровня IT-безопасности, сочетающие мощную защиту от вредоносного программного обеспечения, гибкие инструменты управления, технологии шифрования и средства системного администрирования.

Продукты «Лаборатории Касперского» защищают все узлы корпоративной сети: от рабочих мест до серверов и шлюзов. Используя наш уникальный интегрированный подход, вы сможете контролировать все физические, виртуальные и мобильные устройства и управлять их защитой с помощью единой централизованной консоли администрирования — независимо от размеров вашей IT-инфраструктуры. Технологии «Лаборатории Касперского» входят в состав продуктов и услуг крупнейших мировых производителей и поставщиков IT-решений.

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

Информация об интернет-угрозах: [www.securelist.ru](http://www.securelist.ru)

# ► УНИКАЛЬНАЯ ПЛАТФОРМА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

## ЕДИНАЯ КОНСОЛЬ УПРАВЛЕНИЯ

Администратор может наблюдать за состоянием защиты всех физических, виртуальных и мобильных устройств, а также управлять их безопасностью с помощью единой консоли администрирования.

## ЕДИНАЯ ПЛАТФОРМА

Все используемые в продуктах «Лаборатории Касперского» ключевые технологии, функциональные компоненты и модули разрабатываются внутри компании на собственной технологической базе. Благодаря этому растет эффективность, снижается нагрузка на систему и повышается стабильность работы приложений.

## ЕДИНАЯ ЛИЦЕНЗИЯ

Вы не получаете несколько отдельных решений в рамках одной покупки — вы приобретаете единое комплексное решение, которое вы можете гибко настраивать в соответствии со своими бизнес-целями.

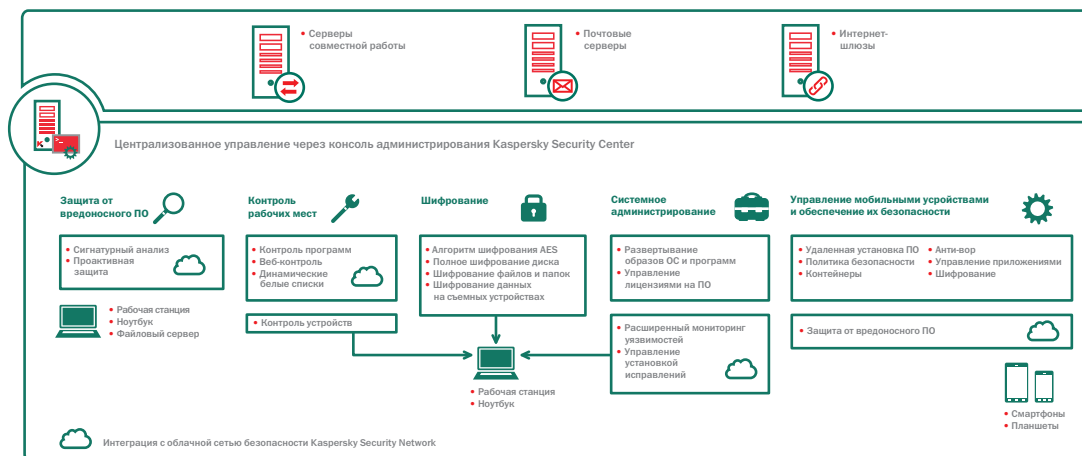
# ► РЕШЕНИЕ, КОТОРОЕ ПОДХОДИТ ИМЕННО ВАМ

Линейка Kaspersky Security для бизнеса позволяет выбрать именно то решение, которое нужно вашей организации, чтобы вы могли контролировать рабочие места (от рабочих станций до смартфонов и виртуальных машин), серверы и интернет-шлюзы и обеспечить их надежной защитой. Наши продукты также позволяют управлять безопасностью всей вашей IT-инфраструктуры удаленно.

«Лаборатория Касперского» обладает обширным набором технологий: от средств шифрования и управления мобильными устройствами до инструментов управления установкой исправлений и использованием лицензий.

Все наши технологии интегрированы между собой и активно взаимодействуют с облачной сетью безопасности Kaspersky Security Network, что позволяет предоставить нашим клиентам защиту мирового класса от становящихся все более сложными современных киберугроз.

Мы разработали уникальную платформу для обеспечения безопасности, которая позволяет администраторам эффективно управлять IT-инфраструктурой и системой ее защиты.



# ► KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Наши технологии на страже вашей IT-инфраструктуры

	СТАРТОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	TOTAL	Управление через Kaspersky Security Center	Можно приобрести в виде отдельного продукта
Защита от вредоносного ПО	•	•	•	•	•	
Сетевой экран	•	•	•	•	•	
Контроль программ		•	•	•	•	
Контроль устройств		•	•	•	•	
Веб-Контроль		•	•	•	•	
Защита файловых серверов		•	•	•	•	•
Защита мобильных устройств		•	•	•	•	•
Управление мобильными устройствами (MDM)		•	•	•	•	•
Шифрование данных			•	•	•	
Развертывание ОС и приложений			•	•	•	•
Управление лицензиями			•	•	•	•
Мониторинг уязвимостей			•	•	•	•
Управление установкой исправлений			•	•	•	•
Контроль доступа в сеть (NAC)			•	•	•	•
Защита серверов совместной работы				•		•
Защита почтовых серверов				•		•
Защита интернет-шлюзов				•		•
Защита виртуальных сред					•	•
Защита систем хранения данных					•	•

# ► KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА



## Kaspersky Endpoint Security для бизнеса — СТАРТОВЫЙ

Это идеальный вариант для заказчиков, которым необходима только защита от вредоносного ПО. Единая консоль управления Kaspersky Security Center с интуитивно понятным интерфейсом дополняет все наши решения для рабочих станций.

## Kaspersky Endpoint Security для бизнеса — СТАНДАРТНЫЙ

Список средств защиты в решении уровня СТАНДАРТНЫЙ включает средства обеспечения безопасности рабочих станций и файловых серверов, динамические белые списки, а также средства контроля программ, устройств и веб-ресурсов. В него также входят инструменты для защиты мобильных устройств и управления ими. Если потребности вашего бизнеса включают защиту мобильных сотрудников и применение политик IT-безопасности, то вам подойдет решение уровня СТАНДАРТНЫЙ.

## Kaspersky Endpoint Security для бизнеса — РАСШИРЕННЫЙ

На уровне РАСШИРЕННЫЙ «Лаборатория Касперского» добавила ко всем вышеперечисленным функциям шифрование данных. Еще одна новая разработка «Лаборатории Касперского» — средство системного администрирования — обеспечивает безопасность и одновременно повышает производительность IT-инфраструктуры. Такой широкий набор функций и полезных инструментов позволяет:

- создавать и хранить образы систем и осуществлять их удаленное развертывание;
- устанавливать приоритет устранения уязвимостей в аппаратном и программном обеспечении благодаря эффективному сочетанию мониторинга уязвимостей и интеллектуального управления установкой исправлений;
- контролировать использование лицензий на программное обеспечение с помощью модуля управления лицензиями;
- задавать политики доступа к данным и IT-инфраструктуре для пользователей и гостей с помощью средства контроля доступа в сеть (NAC);
- удаленно развертывать и устанавливать программы и обновления на компьютеры пользователей с помощью единой централизованной консоли администрирования.

## Kaspersky Total Security для бизнеса

Наш флагманский продукт — Kaspersky Total Security для бизнеса — включает в себя возможности всех предыдущих уровней и дополнительно укрепляет безопасность вашей IT-инфраструктуры с помощью средств для защиты почтовых серверов, интернет-шлюзов и серверов совместной работы. Это идеальное решение для организаций с высокими требованиями к IT-безопасности, которым нужна надежная защита каждого узла сети.

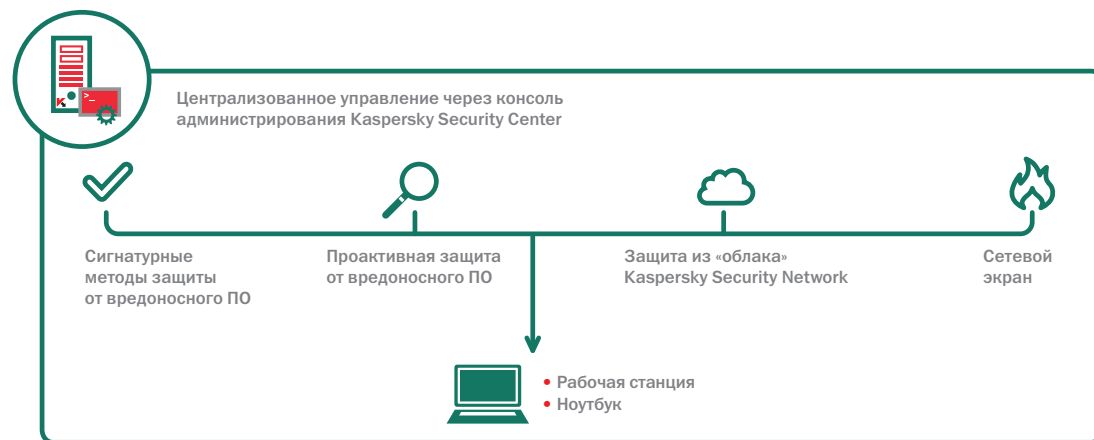
# ▶ KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

## СТАРТОВЫЙ



Высокоэффективное решение для защиты от вредоносных программ с возможностями централизованного развертывания и управления, а также формирования отчетов.

Линейка решений для обеспечения защиты от вредоносных программ начинается с уровня СТАРТОВЫЙ. Kaspersky Endpoint Security для бизнеса СТАРТОВЫЙ управляется централизованно с помощью Kaspersky Security Center и поддерживается облачной сетью безопасности Kaspersky Security Network (KSN).



Примечание: набор доступных функций зависит от защищаемой платформы.

## ОСНОВНЫЕ ВОЗМОЖНОСТИ

**НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО**  
Технологии антивирусной проверки «Лаборатории Касперского» работают на разных уровнях операционной системы, эффективно удаляя вредоносное ПО.

**ЗАЩИТА ИЗ «ОБЛАКА»**  
Благодаря облачной сети Kaspersky Security Network пользователи получают защиту от новых угроз в режиме реального времени.

## ЗАЩИТА РАБОЧИХ МЕСТ

**СИГНАТУРНЫЙ МЕТОД**  
Традиционный метод обнаружения вредоносного программного обеспечения, основанный на использовании сигнатур.

**ПРОАКТИВНАЯ ЗАЩИТА**  
Защита от угроз, для которых еще не созданы сигнатуры.

**СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И ПЕРСОНАЛЬНЫЙ СЕТЕВОЙ ЭКРАН**  
Предустановленные правила для сотен наиболее распространенных приложений позволяют сократить затраты времени на настройку сетевого экрана.

## ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

**ЕДИНАЯ КОНСОЛЬ АДМИНИСТРИРОВАНИЯ**  
Служит для удаленного управления безопасностью всех рабочих мест, защищаемых продуктом «Лаборатории Касперского».

**ИНТУИТИВНО ПОНЯТНЫЙ ИНТЕРФЕЙС**  
Информационная панель позволяет администратору отслеживать состояние защиты в режиме реального времени, применять политики и получать отчеты.

**ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ**  
Администраторы могут удалять имеющееся антивирусное программное обеспечение, устанавливать и настраивать продукты «Лаборатории Касперского», а также создавать отчеты — и все это с помощью единой консоли.

**ЗАЩИТА ИЗ «ОБЛАКА»**  
Облачная сеть безопасности Kaspersky Security Network (KSN) позволяет реагировать на новые угрозы намного быстрее, чем традиционные методы защиты. Время реакции KSN на появление нового вредоносного ПО может составлять всего 0,02 секунды!

**ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ**  
«Лаборатория Касперского» предлагает средства для защиты рабочих мест на базе Windows®, Mac OS и Linux®, что снижает нагрузку на администраторов, обслуживающих мультиплатформенные сети.

**ВЕБ-ИНТЕРФЕЙС**  
Удобный веб-интерфейс служит для удаленного наблюдения за состоянием защиты и просмотра отчетов о ключевых событиях.

**МАСШТАБИРУЕМОСТЬ**  
Kaspersky Security Center обеспечивает развертывание и управление системой защиты, гибкое применение политик и создание подробных отчетов в соответствии с растущими требованиями вашей IT-инфраструктуры независимо от ее масштаба.



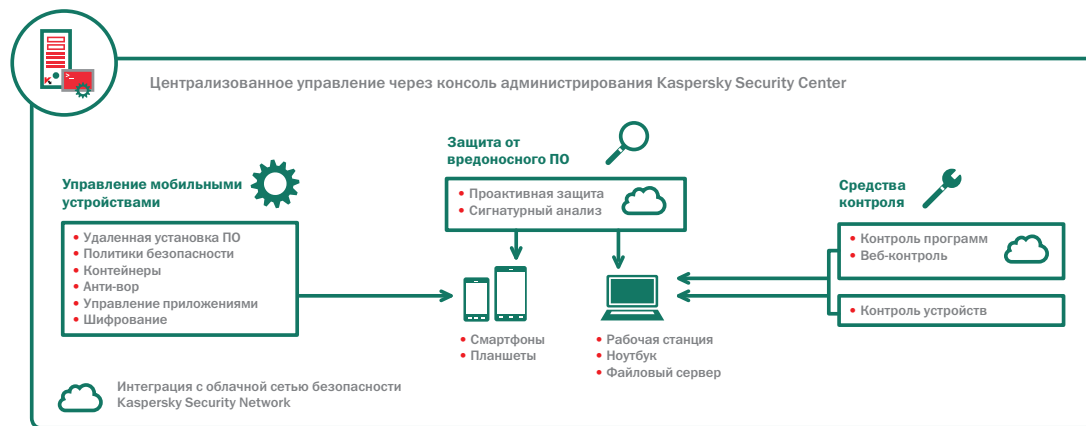
# ▶ KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

## СТАНДАРТНЫЙ



Средства для обеспечения безопасности мобильных сотрудников, эффективное применение политик IT-безопасности и защита от вредоносных программ.

Решение «Лаборатории Касперского» уровня СТАНДАРТНЫЙ включает в себя средства для управления мобильными устройствами и защиты их от вредоносных программ. Средства контроля корпоративных ПК (контроль использования веб-ресурсов, устройств и программ) помогут вашей организации эффективно применять политики, обеспечивающие безопасность важнейших элементов IT-инфраструктуры.



**Примечание:** набор доступных функций зависит от защищаемой платформы.

## ОСНОВНЫЕ ВОЗМОЖНОСТИ

**НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО**  
Технологии антивирусной проверки «Лаборатории Касперского» работают на разных уровнях операционной системы, эффективно удаляя вредоносное ПО. Облачная сеть безопасности Kaspersky Security Network (KSN) защищает пользователей от новых угроз в режиме реального времени.

**ГИБКИЕ СРЕДСТВА КОНТРОЛЯ**  
Облачная база опасных и легитимных программ и веб-сайтов помогает администратору создавать и применять политики доступа к программам и веб-страницам. При этом гибкие средства контроля позволяют гарантировать, что к компьютерам в сети будут подключены только разрешенные устройства.

## КОНТРОЛЬ РАБОЧИХ МЕСТ

**КОНТРОЛЬ ПРОГРАММ**  
Позволяет системным администраторам задавать политики, которые разрешают, блокируют или ограничивают использование определенных программ (или категорий программ).

**ДИНАМИЧЕСКИЕ БЕЛЫЕ СПИСКИ**  
Репутационная проверка файлов в режиме реального времени по базе Kaspersky Security Network (KSN) позволяет гарантировать, что доверенные приложения не содержат вредоносного кода.

## ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

**ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПО**  
Защита в режиме реального времени возможна благодаря сочетанию сигнатурных, проактивных и облачных технологий. Безопасный браузер, защита от спама и технология Sandbox для безопасного запуска приложений повышают уровень защиты.

**УДАЛЕННАЯ УСТАНОВКА ПО**  
Возможность предварительной настройки и дальнейшей централизованной установки приложений на мобильные устройства с помощью SMS, электронной почты или ПК.

**ЗАЩИТА ЦЕННЫХ ДАННЫХ**  
Функции поиска, удаленной блокировки устройства и стирания данных на нем, а также SIM-Контроль служат для предотвращения

**БЕЗОПАСНОСТЬ СМАРТФОНОВ И ПЛАНШЕТОВ**  
Защита на основе программных агентов доступна для устройств под управлением Android™, BlackBerry®, Symbian и Windows® Mobile. С помощью средства управления мобильными устройствами (Mobile Device Management) политики и приложения легко устанавливаются по беспроводным каналам связи на мобильные устройства, в том числе на устройства под управлением iOS.

**ВЕБ-КОНТРОЛЬ**  
Обеспечивает контроль использования веб-ресурсов независимо от того, находится пользователь в пределах корпоративной сети или нет.

**КОНТРОЛЬ УСТРОЙСТВ**  
Позволяет администратору создавать и применять (в том числе по расписанию) политики работы с данными на съемных носителях и других периферийных устройствах, подключаемых через USB или любой другой интерфейс.

несанкционированного доступа к корпоративным данным при утере или краже мобильного устройства.

**КОНТРОЛЬ ПРИЛОЖЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ**  
Позволяет осуществлять мониторинг приложений на корпоративных мобильных устройствах в соответствии с групповыми политиками безопасности.

**ЗАЩИТА ЛИЧНЫХ УСТРОЙСТВ СОТРУДНИКОВ**  
В вашей компании приветствуется работа на личных устройствах? Корпоративные данные и приложения могут быть помещены в изолированные зашифрованные контейнеры, «прозрачные» для пользователя. Данные в таком контейнере можно удалить независимо от других данных, хранящихся на устройстве.

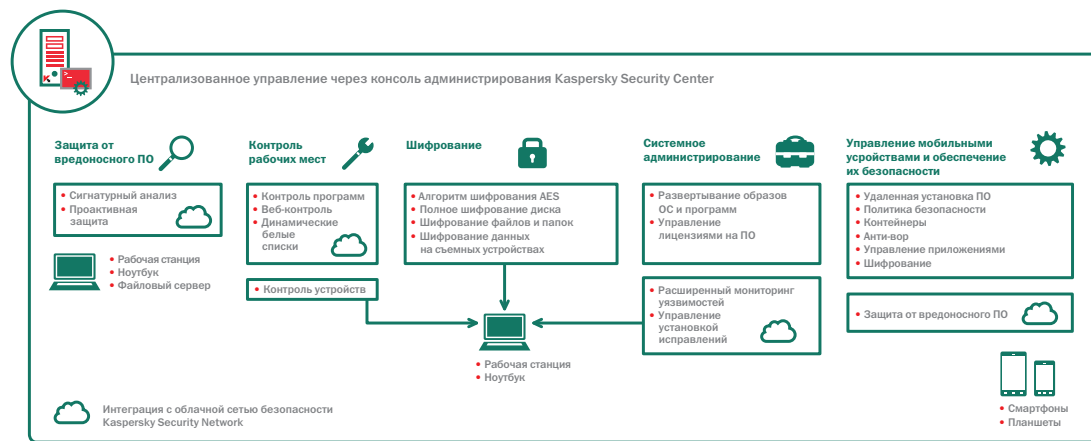
# ► KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

## РАСШИРЕННЫЙ



В линейке решений «Лаборатории Касперского» эффективно сочетаются технологии обеспечения безопасности и инструменты управления IT-инфраструктурой.

Решение «Лаборатории Касперского» уровня РАСШИРЕННЫЙ предоставляет возможности защиты и управления, необходимые вашей организации для внедрения политик IT-безопасности, защиты от вредоносного программного обеспечения и потери данных, а также для повышения производительности корпоративной IT-инфраструктуры.



Примечание: набор доступных функций зависит от защищаемой платформы.

## ОСНОВНЫЕ ВОЗМОЖНОСТИ

### ШИФРОВАНИЕ ДАННЫХ

Защита ценных корпоративных данных в случае кражи или утери устройства, на котором они хранятся. Для этого можно использовать как полное шифрование диска, так и шифрование отдельных файлов и папок — с помощью алгоритма Advanced Encryption Standard (AES).

### КОНТРОЛЬ И ЗАЩИТА РАБОЧИХ МЕСТ

Сочетание сигнатурных, проактивных и облачных методов защиты от вредоносного ПО, а также гибкие инструменты контроля рабочих мест: Контроль программ, Контроль устройств и Веб-Контроль.

## ШИФРОВАНИЕ И ЗАЩИТА ДАННЫХ

### ПОЛНОЕ ИЛИ ВЫБОРОЧНОЕ ШИФРОВАНИЕ ДАННЫХ

Чтобы защитить ценные корпоративные данные в случае кражи или утери устройства, на котором они хранятся, можно использовать как полное шифрование диска, так и шифрование отдельных файлов и папок — с помощью алгоритма Advanced Encryption Standard (AES).

### ШИФРОВАНИЕ ДАННЫХ НА СЪЕМНЫХ НОСИТЕЛЯХ

Политики шифрования данных на съемных носителях позволяют повысить уровень безопасности.

### СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Инструменты для развертывания образов ОС и программ, контроля доступа в сеть, управление лицензиями и установка исправлений доступны в единой консоли администрирования Kaspersky Security Center.

### УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ И ИХ ЗАЩИТА

Развертывание, администрирование и защита мобильной IT-инфраструктуры компании, а также защита корпоративных данных, хранящихся на личных устройствах пользователей.

### БЕЗОПАСНОЕ СОВМЕСТНОЕ ПОЛЬЗОВАНИЕ ДАННЫМИ

Пользователи могут легко создавать зашифрованные самораспаковывающиеся контейнеры, чтобы обеспечить защиту данных, передаваемых на съемных носителях, по электронной почте, через локальную сеть или интернет.

### НЕЗАМЕТНОСТЬ ДЛЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

Наши технологии шифрования работают незаметно для пользователей и не снижают производительность системы.

## ИНСТРУМЕНТЫ СИСТЕМОГО АДМИНИСТРИРОВАНИЯ

### УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ

Расширенный мониторинг уязвимостей в сочетании с автоматическим распределением исправлений (патчей).

### РАЗВЕРТЫВАНИЕ ОБРАЗОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММ

Простой централизованный процесс создания, хранения и развертывания образов ОС и программ. Идеально подходит для миграции на Microsoft® Windows® 8.

### УДАЛЕННАЯ УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Централизованная установка программного обеспечения на клиентские компьютеры, в том числе в филиалах организации.

### КОНТРОЛЬ ДОСТУПА В СЕТЬ (НАС)

Возможность создать политику для подключающихся к корпоративной сети гостей. Гостевые устройства (в том числе мобильные) автоматически распознаются и перенаправляются на корпоративный портал, где пользователи вводят выданные им идентификационные пароли и получают доступ к разрешенным ресурсам.

### УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ, УЧЕТ ОБОРУДОВАНИЯ И ПО

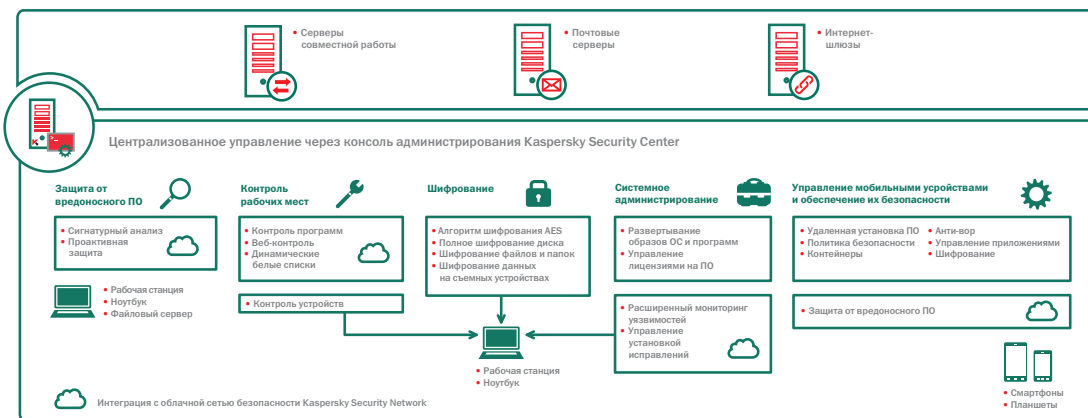
Сводные отчеты об аппаратном и программном обеспечении помогают контролировать статус лицензий на ПО.

# ► KASPERSKY TOTAL SECURITY ДЛЯ БИЗНЕСА



Инструменты шифрования, средства для управления IT-инфраструктурой, возможность создания и эффективного применения политик IT-безопасности, а также надежная защита от вредоносного ПО.

Продукт Kaspersky Total Security для бизнеса является наиболее многофункциональным решением для защиты корпоративной IT-инфраструктуры и управления ею. Решение обеспечивает безопасность всех узлов сети и включает в себя эффективные средства настройки, благодаря чему корпоративные пользователи имеют возможность продуктивно работать, будучи защищенными от всех современных угроз — независимо от своего местонахождения и используемого устройства.



Примечание: набор доступных функций зависит от защищаемой платформы.

## ЗАЩИТА СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ, ПОЧТОВЫХ СЕРВЕРОВ И ИНТЕРНЕТ-ШЛЮЗОВ

### ЗАЩИТА ПОЧТОВЫХ СЕРВЕРОВ

Защита почты для последних версий основных почтовых серверов и серверов совместной работы, таких как Microsoft® Exchange, IBM® Lotus® Domino®, а также почтовых серверов на базе Linux® от вредоносного ПО и спама.

### ЗАЩИТА СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Решение «Лаборатории Касперского» защищает серверы SharePoint® от вредоносного ПО, а средства фильтрации контента и файлов помогают избежать хранения нежелательного контента.

### ЗАЩИТА ИНТЕРНЕТ-ШЛЮЗОВ

Безопасный доступ в интернет для всех сотрудников организации благодаря автоматическому удалению вредоносных и потенциально опасных программ в трафике HTTP(S), FTP, SMTP и POP3.

## ЗАЩИТА И КОНТРОЛЬ РАБОЧИХ МЕСТ

### НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Доказавшие свою эффективность методы обнаружения вредоносного ПО: сочетание сигнатурных, проактивных и облачных технологий.

### КОНТРОЛЬ УСТРОЙСТВ

Позволяет администратору создавать и применять (в том числе по расписанию) политики работы с данными на съемных носителях и других периферийных устройствах, подключаемых через USB или любой другой интерфейс.

### КОНТРОЛЬ ПРОГРАММ

Позволяет системным администраторам задавать политики, которые разрешают, блокируют или ограничивают использование определенных программ (или категорий программ).

### ВЕБ-КОНТРОЛЬ

Обеспечивает контроль использования веб-ресурсов независимо от того, находится пользователь в пределах корпоративной сети или нет.

## ИНСТРУМЕНТЫ СИСТЕМНОГО АДМИНИСТРИРОВАНИЯ

### УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ

Расширенный мониторинг уязвимостей в сочетании с автоматическим распределением исправлений (патчей).

### РАЗВЕРТЫВАНИЕ ОБРАЗОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММ

Простой централизованный процесс создания, хранения и развертывания образов ОС и программ. Идеально подходит для миграции на Microsoft Windows® 8.

### КОНТРОЛЬ ДОСТУПА В СЕТЬ (НАС)

Возможность создать политику для подключающихся к корпоративной сети гостей. Гостевые устройства (в том числе мобильные) автоматически распознаются и перенаправляются на корпоративный портал, где пользователи вводят выданные им идентификационные пароли и получают доступ к разрешенным ресурсам.

### УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ, УЧЕТ ОБОРУДОВАНИЯ И ПО

Сводные отчеты об аппаратном и программном обеспечении помогают контролировать статус лицензий на ПО.

## ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

### УДАЛЕННАЯ УСТАНОВКА ПО

Возможность предварительной настройки и дальнейшей централизованной установки приложений на мобильные устройства с помощью SMS, электронной почты или ПК.

### КОНТРОЛЬ ПРИЛОЖЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Позволяет осуществлять мониторинг приложений на корпоративных мобильных устройствах в соответствии с групповыми политиками безопасности.

### ЗАЩИТА ЦЕННЫХ ДАННЫХ

Функции поиска, удаленной блокировки устройства и стирания данных на нем, а также SIM-Контроль служат для предотвращения несанкционированного доступа к корпоративным данным при утере или краже мобильного устройства.

### ЗАЩИТА ЛИЧНЫХ УСТРОЙСТВ СОТРУДНИКОВ

В вашей компании приветствуется работа на личных устройствах? Корпоративные данные и приложения могут быть помещены в изолированные зашифрованные контейнеры, прозрачные для пользователя. Данные в таком контейнере можно удалить независимо от других данных, хранящихся на устройстве.



# ► KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Простое управление мобильными устройствами и высочайший уровень их защиты в отсутствие сложностей, связанных с использованием специализированного решения.

Развертывание, администрирование и защита мобильной IT-инфраструктуры не обязательно должны быть сложными или дорогостоящими. Модуль управления мобильными устройствами делает настройку системы безопасности простой и удобной. А специальное мобильное приложение, устанавливаемое на устройства, обеспечивает надежную защиту от всех современных угроз. Мобильное приложение можно также установить на личные устройства сотрудников.

## ЭФФЕКТИВНОЕ АДМИНИСТРИРОВАНИЕ

**ПРОСТАЯ НАСТРОЙКА С ПОМОЩЬЮ ЕДИНОЙ КОНСОЛИ**  
В отличие от решений других производителей, продукт «Лаборатории Касперского» позволяет администраторам использовать единую консоль для управления безопасностью мобильных устройств, физических рабочих мест и виртуальных систем, а также шифрованием и применением политик.

### ЦЕНТР ЗАГРУЗКИ ПРИЛОЖЕНИЙ

Администраторы могут создать корпоративный портал, содержащий ссылки на разрешенные к использованию приложения, и с помощью специальной политики обязать пользователей работать только с ними.

### УДАЛЕННАЯ УСТАНОВКА ПО

Администратор может обеспечить безопасность телефонов удаленно, разослав сотрудникам электронные сообщения или

SMS, содержащие ссылку на корпоративный портал, с которого пользователям следует загрузить одобренные настройки и приложения. До тех пор пока пользователь не сделает этого, доступ к корпоративным данным для него будет закрыт.

### НАСТРОЙКА ПАРАМЕТРОВ ЗАЩИТЫ

Для сохранения целостности аппаратного и программного обеспечения предусмотрена регистрация попыток несанкционированной перепрошивки. Среди других параметров защиты — отключение камеры, защита паролем и многое другое.

### ПРИМЕНЕНИЕ ПОЛИТИК

Функция контроля программ позволяет отслеживать и контролировать использование приложений на устройстве, в том числе с помощью режимов «Запрет по умолчанию» и «Разрешение по умолчанию».

## ИНСТРУМЕНТЫ ЗАЩИТЫ

### ШИФРОВАНИЕ

Защита данных на мобильных устройствах осуществляется с помощью прозрачного для пользователя шифрования на уровне диска или отдельных файлов и папок, которое также может быть применено к контейнерам.

### АНТИ-ВОР

Администраторы могут удаленно выполнять полное или частичное удаление данных с устройств, определять местонахождение пропавших устройств с помощью функции

GPS-Поиск, а также получать уведомления при извлечении или замене SIM-карты.

### ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Защиту устройств от вредоносных программ обеспечивают антивирусное ядро «Лаборатории Касперского», включающее несколько уровней обнаружения вредоносного ПО, в том числе с использованием «облака», а также безопасный браузер и эффективные средства борьбы со спамом.

## ЗАЩИТА КОРПОРАТИВНЫХ ДАННЫХ

### КОНТЕЙНЕРЫ

В том случае, если сотрудники используют для работы личные устройства, корпоративные данные и приложения можно помещать в изолированные контейнеры. Эта мера обеспечивает максимальную безопасность корпоративных данных и хранение их отдельно от личной информации пользователей.

### СРЕДСТВА ДЛЯ УДАЛЕННОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

В случае утери или кражи устройства его можно удаленно заблокировать. Корпоративные данные внутри контейнера можно зашифровать или удаленно стереть с устройства, не затрагивая при этом личные данные пользователя.



- Корпоративные данные хранятся отдельно
- Данные зашифрованы
- Данные можно выборочно стереть

## ИДЕАЛЬНОЕ РЕШЕНИЕ ДЛЯ ЛИЧНЫХ УСТРОЙСТВ, ИСПОЛЗУЕМЫХ В РАБОЧИХ ЦЕЛЯХ

Зачастую сотрудники используют собственные устройства одновременно в личных и в служебных целях. В некоторых организациях сотрудники самостоятельно приобретают смартфон или планшет, который им нравится, а IT-служба затем настраивает на нем электронную почту и доступ к корпоративным ресурсам.

С одной стороны, это приводит к сокращению затрат и повышению производительности труда, с другой — создает дополнительные риски безопасности. Корпоративные данные, не защищенные должным образом (и, возможно, смешанные с личными данными пользователя), легко могут стать добычей злоумышленников. Часто теми же устройствами пользуются члены семей сотрудников, не задумывающиеся о вопросах безопасности. Иногда на них даже открывают root-доступ или меняют прошивку.

Kaspersky Security для мобильных устройств успешно решает эти проблемы, позволяя настроить параметры безопасности на смартфонах и планшетах с помощью единой консоли, которая используется для обеспечения безопасности всей корпоративной сети. Вы можете быть уверены, что на устройствах пользователей заданы требуемые параметры и что ценные корпоративные данные будут защищены в случае утери, кражи или ненадлежащего использования устройства владельцами.



**Примечание:** набор доступных функций зависит от защищаемой платформы.

# KASPERSKY SYSTEMS MANAGEMENT

Повышение производительности и безопасности IT-инфраструктуры благодаря централизованному управлению настройками и установкой исправлений.

Необходимость защиты данных и поддержки пользователей ставит перед IT-специалистами множество непростых задач. К сожалению, нередко для решения каждой задачи требуется отдельное приложение или инструмент — каждый раз от нового поставщика. По мнению IT-специалистов, одной из основных сложностей, с которыми им приходится сталкиваться, является работа с приложениями, созданными без расчета на взаимодействие друг с другом.

## ИСПОЛЬЗОВАНИЕ НЕСКОЛЬКИХ ОТДЕЛЬНЫХ РЕШЕНИЙ ПОРОЖДАЕТ ДОПОЛНИТЕЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Представляем вам Kaspersky Systems Management. Это решение предлагает широкий набор мощных инструментов для повышения эффективности работы IT-инфраструктуры компании. Продукт обеспечивает желаемый уровень простоты и автоматизации в сочетании с необходимой защитой и контролем.

### Экономия ресурсов

Вам не придется тратить силы на индивидуальную настройку систем для новых и уже существующих пользователей. Технология развертывания систем на рабочих местах позволяет централизованно создавать и развертывать образы ОС и программ, а также управлять ими.

### Повышение уровня безопасности

Установка исправлений (патчей) в корпоративной IT-инфраструктуре может занимать до нескольких дней. Решение «Лаборатории Касперского» позволяет справиться с этой задачей намного быстрее. Продукт идентифицирует уязвимости, которые могут быть использованы злоумышленниками, и позволяет указать, какие уязвимости нужно устранить в первую очередь, а какие можно закрыть по окончании рабочего дня. Расстановка приоритетов помогает администраторам эффективно использовать свое время, уделяя больше внимания повышению уровня безопасности.

### Высокая эффективность работы

Администраторы могут удаленно устанавливать образы, обновления, исправления и программы. Если у пользователя возникает проблема, IT-специалист может дистанционно подключиться к его компьютеру и устранить неполадки в системе. Благодаря этому администратор не теряет времени на перемещение между рабочими местами или на малоэффективное решение проблем по телефону.

Доступ к этим и другим функциям Kaspersky Systems Management осуществляется через единую консоль управления Kaspersky Security Center. Поскольку отсутствует необходимость в использовании отдельной консоли для каждого компонента, система управления отличается последовательностью и простотой и не требует дополнительного обучения.

## ИНСТРУМЕНТЫ СИСТЕМНОГО АДМИНИСТРИРОВАНИЯ

**РАЗВЕРТЫВАНИЕ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ**  
Простое централизованное создание, хранение, копирование и развертывание образов систем позволяет обеспечить эффективную установку систем с оптимальными параметрами безопасности. Идеально подходит для миграции на Microsoft® Windows® 8.

### МОНИТОРИНГ УЯЗВИМОСТЕЙ

Проверка аппаратного и программного обеспечения на уязвимости, запускаемая одним кликом мыши, производится по нескольким базам уязвимостей. Вы можете определить, какие из обнаруженных уязвимостей требуют немедленного внимания, а для каких установку исправлений можно отложить до конца рабочего дня.

### УДАЛЕННАЯ УСТАНОВКА ПО

Минимизация нагрузки на сеть за счет удаленного развертывания ПО по расписанию или вручную.

### УДАЛЕННЫЕ АГЕНТЫ ОБНОВЛЕНИЙ

Вы можете назначить рабочую станцию в удаленном офисе или филиале центральным агентом обновлений. Это позволяет сократить нагрузку на сеть: в удаленный офис направляется одно обновление, а назначенный центральным агентом компьютер используется для распространения обновления по локальной сети.

### ПОДДЕРЖКА ТЕХНОЛОГИИ WAKE-ON-LAN

Для выполнения действий по развертыванию и поддержке в нерабочее время Kaspersky Systems Management позволяет удаленно включать рабочие станции.

### СРЕДСТВА УСТРАНЕНИЯ НЕПОЛАДОК

Для устранения неполадок можно безопасно дистанционно подключиться к компьютеру пользователя с помощью единой консоли управления.

### КОНТРОЛЬ ДОСТУПА В СЕТЬ (НАС)

Возможность создать политику для подключающихся к корпоративной сети гостей. Гостевые устройства (в том числе мобильные) автоматически распознаются и перенаправляются на корпоративный портал, где пользователи вводят выданные им идентификационные пароли и получают доступ к разрешенным вами ресурсам.

### ПОДДЕРЖКА MICROSOFT WSUS

Kaspersky Systems Management регулярно выполняет синхронизацию данных с серверами, в том числе с центром обновления Microsoft Windows. Информация о доступных обновлениях и исправлениях затем загружается при помощи служб Windows Server Update Services и распространяется по сети оптимальным образом.

### УЧЕТ АППАРАТНОГО ОБЕСПЕЧЕНИЯ

Обнаружение и учет компьютеров и подключаемых внешних устройств происходит автоматически. При появлении в корпоративной сети нового устройства администратору отправляется соответствующее уведомление. Эта функция позволяет отслеживать использование оборудования в сети.

### УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ

Kaspersky Systems Management ведет учет того, какое именно программное обеспечение используется в вашей IT-инфраструктуре. Это позволяет оптимизировать затраты на лицензирование и выявлять пользователей, не соблюдающих требования. При развертывании с помощью средств системного администрирования «Лаборатории Касперского» вы можете указать разрешенное к установке и использованию ПО, а также ограничить количество лицензий.

# ► KASPERSKY SECURITY ДЛЯ ФАЙЛОВЫХ СЕРВЕРОВ

Kaspersky Security для файловых серверов — это решение, обеспечивающее надежную защиту файловых серверов под управлением операционных систем Windows®, Windows Server® Enterprise Edition и Linux от всех видов вредоносных программ.

Антивирусная защита сетевых хранилищ общего доступа очень важна, поскольку один-единственный зараженный файл на сервере может стать источником заражения компьютеров всех пользователей, обращающихся к ресурсу. Хорошо продуманная защита файлового сервера не только обеспечивает безопасную работу пользователей с данными и сохранность важной информации, но и позволяет избежать попадания вредоносных программ в резервные копии данных, что может стать причиной повторных вирусных эпидемий и других проблем.

## ОСОБЕННОСТИ

- комплексная защита файловых серверов в гетерогенных сетях
- оптимальное использование системных ресурсов
- сертификат VMware Ready

## ФУНКЦИИ

- защита файловых серверов под управлением Windows, Windows Server® Enterprise Edition, Linux и Free BSD
- расширенная проактивная защита от новых вредоносных программ
- антивирусная защита в режиме реального времени
- проверка файловых хранилищ по расписанию
- проверка критических областей системы
- масштабируемость
- карантинное хранилище для подозрительных объектов
- резервное копирование данных перед их лечением / удалением

## АДМИНИСТРИРОВАНИЕ

- централизованная установка, управление и обновление
- выбор способа установки и управления приложением
- система уведомлений о работе приложения
- гибкая система настроек проверки и реагирования на инциденты
- система отчетов о состоянии защиты

**Примечание:** набор доступных функций зависит от защищаемой платформы.

# ► KASPERSKY SECURITY ДЛЯ ПОЧТОВЫХ СЕРВЕРОВ

Kaspersky Security для почтовых серверов — это решение для защиты почтовых серверов от вредоносных программ и спама.

Продукт включает приложения для защиты всех популярных почтовых серверов — Microsoft® Exchange, Lotus® Domino®, Sendmail, qmail, Postfix и Exim, а также позволяет организовать выделенный почтовый шлюз.

## ОСОБЕННОСТИ

- поддержка последних версий Microsoft Exchange Server и IBM® Lotus® Domino®
- эффективная защита от спама
- оптимальное использование системных ресурсов
- простой и удобный механизм обновления антивирусных и антиспам-баз
- система разделения прав администраторов
- сертификат VMware Ready

## ФУНКЦИИ

- комплексная защита почтовых серверов от вредоносных программ
- эффективная защита от спама и целевых атак
- антивирусная защита в режиме реального времени
- проверка почтовых сообщений и баз данных по расписанию
- обработка сообщений, баз данных и других объектов на серверах Lotus Domino
- проверка всех сообщений на сервере Microsoft Exchange, в том числе в общих папках
- защита почтовых серверов Sendmail, qmail, Postfix и Exim
- масштабируемость
- поддержка кластерных конфигураций для Microsoft Exchange Server 2007 и поддержка DAG для Microsoft Exchange Server 2010
- фильтрация сообщений в зависимости от типов вложений
- карантинное хранилище для подозрительных объектов
- резервное копирование сообщений перед их лечением / удалением
- исключение повторных проверок сообщений
- репутационная фильтрация почтового трафика

## АДМИНИСТРИРОВАНИЕ

- удобные инструменты установки, управления и обновления
- гибкая система настроек проверки и реагирования на инциденты
- система уведомлений о работе приложения
- система отчетов о состоянии защиты

**Примечание:** набор доступных функций зависит от защищаемой платформы.

# ► KASPERSKY SECURITY ДЛЯ ИНТЕРНЕТ-ШЛЮЗОВ

Решение Kaspersky Security для интернет-шлюзов обеспечивает всем пользователям корпоративной сети безопасный доступ в интернет.

Kaspersky Security для интернет-шлюзов поддерживает все основные версии сетевых экранов. Вредоносные и потенциально опасные программы автоматически удаляются из потока данных, передаваемых по протоколам HTTP, HTTPS, FTP, POP3 и SMTP. Технологии оптимизации работы приложений, масштабируемость и поддержка современных аппаратных платформ позволяют использовать продукт в крупных организациях с большим объемом трафика.

## ОСОБЕННОСТИ

- защита сервера Microsoft® Forefront® TMG
- широкие возможности настроек и управления политиками
- проверка VPN-соединений
- мониторинг работы приложения для Microsoft ISA Server и Forefront® TMG)
- защита почтового трафика, проходящего по протоколам POP3 и SMTP
- проверка HTTP- и FTP-трафика, поступающего на опубликованные серверы
- сертификат VMware Ready

## ФУНКЦИИ

- проверка трафика, проходящего по протоколам HTTP, HTTPS, FTP, POP3 и SMTP, в режиме реального времени
- комплексная защита от всех типов вредоносных программ
- выявление потенциально опасных программ
- поддержка прокси-серверов Squid, Blue Coat, Cisco®
- резервное копирование данных
- распределение нагрузки между процессорами сервера
- масштабируемость

## АДМИНИСТРИРОВАНИЕ

- удобные инструменты установки, управления и обновления
- гибкая система настроек проверки
- система отчетов и оповещений о состоянии защиты

**Примечание:** набор доступных функций зависит от защищаемой платформы.

# ► KASPERSKY SECURITY ДЛЯ СЕРВЕРОВ СОВМЕСТНОЙ РАБОТЫ

Kaspersky Security для серверов совместной работы — специализированное защитное решение на базе последнего антивирусного ядра «Лаборатории Касперского», предназначенное для серверов SharePoint®.

Чтобы обеспечить безопасную и бесперебойную совместную работу, «Лаборатория Касперского» разработала решение, в котором сочетаются простота управления, высокий уровень обнаружения угроз и низкая совокупная стоимость владения.

## ОСОБЕННОСТИ

### ЗАЩИТА ОТ ВРЕДНОСНОГО ПО

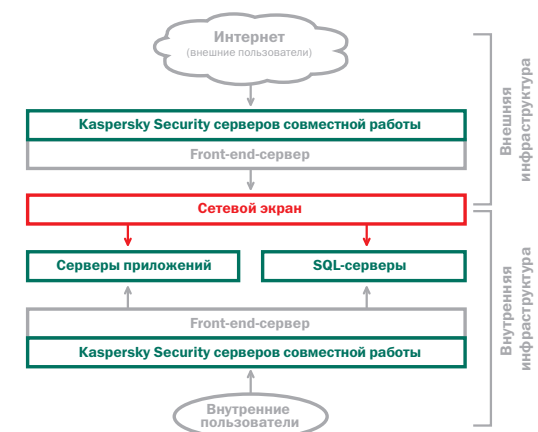
Новое антивирусное ядро «Лаборатории Касперского» и регулярные обновления баз обеспечивают высочайший уровень детектирования вредоносного ПО. Kaspersky Security для серверов совместной работы защищает всю ферму серверов SharePoint, включая front-end-сервер, SQL Server®, серверы приложений и индексирования, поисковый сервер и т.д.

### ПОЛИТИКИ ДОКУМЕНТООБОРОТА

Благодаря функциям фильтрации контента весь документооборот на сайтах SharePoint осуществляется в соответствии с принятыми в компании политиками и стандартами. Kaspersky Security для серверов совместной работы позволяет предотвратить хранение файлов с ненадлежащим контентом.

### ПРОСТОЕ УПРАВЛЕНИЕ

Вся ферма серверов может управляться централизованно из единой консоли с интуитивно понятным интерфейсом, которая включает все наиболее распространенные сценарии администрирования.



# ► KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Kaspersky Security для виртуальных сред специально разработан с учетом особенностей виртуальной IT-инфраструктуры. Это решение обеспечивает высочайший уровень защиты для виртуальных сред на базе VMware ESXi, Microsoft® Hyper-V и Citrix Xen.

Kaspersky Security для виртуальных сред — это гибкое решение для защиты виртуальной инфраструктуры и повышения ее производительности.

## ФУНКЦИИ

- Централизованная защита VM с помощью виртуального устройства безопасности
- Расширенная защита от вредоносного ПО
- Персональный сетевой экран и система предотвращения вторжений (HIPS)
- Контроль приложений, веб-ресурсов и периферийных устройств
- Интеграция с облачной сетью безопасности Kaspersky Security Network (KSN)
- Блокирование сетевых атак
- Антифишинг
- Проверка IM-сообщений, почтовый и веб-антивирус
- Централизованное управление через Kaspersky Security Center

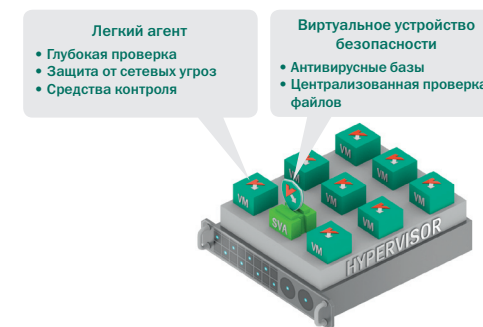
## ГИБКОЕ ЛИЦЕНЗИРОВАНИЕ

Kaspersky Security для виртуальных сред может лицензироваться двумя способами, в зависимости от ваших потребностей:

- По количеству виртуальных машин:
  - по количеству рабочих станций
  - по количеству серверов
- По количеству ядер физических процессоров

## РАСШИРЕННАЯ ЗАЩИТА НА БАЗЕ ЛЕГКОГО АГЕНТА

Kaspersky Security для виртуальных сред предусматривает два варианта развертывания. Легкий агент, устанавливаемый на каждую виртуальную машину, позволяет использовать расширенный функционал для обеспечения безопасности VM, в том числе мониторинг уязвимостей, контроль программ, устройств и веб-контроль, проверку IM-сообщений, почтовый и веб-антивирус, а также передовые эвристические методы защиты. Вместе эти компоненты образуют мощную многоуровневую систему безопасности, не оказывающую негативного влияния на производительность виртуальной среды.

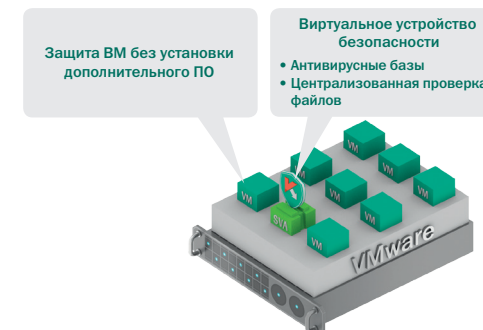


Kaspersky Security для виртуальных сред  
Конфигурация с установкой Легкого агента

## ЗАЩИТА БЕЗ АГЕНТА ДЛЯ СРЕД VMWARE

Тесная интеграция с технологиями VMware позволяет легко развертывать решение Kaspersky Security для виртуальных сред и управлять им на этой платформе без установки агента. Все действия по обеспечению безопасности осуществляются на выделенном виртуальном устройстве, которое взаимодействует с vShield для мгновенной автоматической защиты виртуальных машин, а также с vCloud для обеспечения защиты на уровне сети.

В этой конфигурации недоступны расширенные функции защиты, такие как карантин для подозрительных файлов, HIPS, проверка на наличие уязвимостей и средства контроля.



Kaspersky Security для виртуальных сред  
Конфигурация без агента

## ВИРТУАЛЬНОЕ УСТРОЙСТВО БЕЗОПАСНОСТИ

Оба варианта установки Kaspersky Security для виртуальных сред предполагают использование виртуального устройства безопасности, которое обеспечивает централизованную проверку всех виртуальных машин, размещенных на хост-сервере. Это позволяет эффективно защищать виртуальные машины без дополнительной нагрузки на гипервизор и сохраняет высокую плотность VM. Благодаря такому подходу исключаются ситуации «шквального» обновления и сканирования, а также появления «окна уязвимости» при выходе VM из спящего режима.



# ▶ KASPERSKY SECURITY ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

Kaspersky Security для систем хранения данных защищает сетевые системы хранения данных EMC® VNX™ и NetApp от всех видов вредоносных программ.

Системы хранения данных предоставляют сотрудникам организации любого масштаба удобный и быстрый совместный доступ к информации через корпоративную сеть. Однако в незащищенной корпоративной сети доступ к совместно используемым файлам может привести к негативным последствиям. Единственный зараженный объект из сетевого хранилища способен инфицировать большое число компьютеров и нанести значительный ущерб финансам и репутации компании. Поэтому сетевые системы хранения данных особенно нуждаются в полноценной защите.

Решение Kaspersky Security для систем хранения данных предлагает надежную, высокоэффективную и масштабируемую защиту ценных корпоративных данных, хранящихся в системах EMC VNX и NetApp.

## ФУНКЦИИ

- защита систем хранения данных EMC VNX и NetApp
- поддержка Windows Server® 2008/2012 R2
- поддержка систем иерархического управления запоминающими устройствами (HSM)
- расширенная проактивная защита от новых вредоносных программ
- антивирусная защита в режиме реального времени
- проверка файловых хранилищ по расписанию
- проверка критических областей системы
- оптимальное использование ресурсов
- масштабируемость и отказоустойчивость
- карантинное хранилище для подозрительных объектов
- резервное копирование данных перед их лечением / удалением
- сертификат совместимости VMware
- защита виртуальных систем и терминальных серверов
- поддержка протоколов SNMP/MOM

## АДМИНИСТРИРОВАНИЕ

- централизованная установка, управление и обновление
- система отчетов о состоянии защиты
- система уведомлений о работе приложения
- гибкая настройка параметров проверки

**Примечание:** набор доступных функций зависит от защищаемой платформы.

# ▶ KASPERSKY SMALL OFFICE SECURITY

Kaspersky Small Office Security — это инновационные технологии защиты мирового класса в сочетании с простотой установки и настройки и удобством использования.

Сегодня, когда в компаниях повсеместно используются компьютеры и интернет, IT-инфраструктура небольших предприятий крайне уязвима перед вредоносным ПО и атаками киберпреступников. Под угрозой оказывается вся важная информация, в том числе финансовые онлайн-транзакции и конфиденциальные данные. Небольшим компаниям угрожают те же риски безопасности, что и крупным организациям, однако у малого бизнеса не всегда есть время и ресурсы, чтобы установить и настроить сложные решения для обеспечения IT-безопасности, а затем управлять ими.

Kaspersky Small Office Security обеспечит надежную защиту ваших компьютеров и файловых серверов под управлением Windows®, а также смартфонов и планшетов на базе Android™. С Kaspersky Small Office Security вы можете быть уверены в безопасности проведения банковских операций в интернете, а также в сохранности ваших бизнес-данных и конфиденциальной информации.

## ФУНКЦИИ

- **Защита мирового класса** — многоуровневая защита бизнеса от новейшего вредоносного ПО
- **Интернет-безопасность** — блокирование фишинговых атак и эксплойтов
- **Безопасность мобильных устройств** — технологии защиты устройств Android от вредоносного ПО и модуль Анти-Вор для защиты устройства в случае потери или кражи
- **Менеджер паролей** — создание надежных, устойчивых ко взлому паролей и управление ими.
- **Защита банковских операций в интернете** — технология «Безопасные платежи» для обеспечения безопасности финансовых операций онлайн
- **Защита бизнес-данных** — шифрование данных и локальное/сетевое резервное копирование для обеспечения сохранности важных для бизнеса данных в случае потери, кражи или повреждения устройства

ЗАО «Лаборатория Касперского», Москва, Россия  
[www.kaspersky.ru](http://www.kaspersky.ru)

Всё об интернет-безопасности:  
[www.securelist.ru](http://www.securelist.ru)

Купить в вашем городе:  
[www.kaspersky.ru/find\\_partner\\_office](http://www.kaspersky.ru/find_partner_office)

© ЗАО «Лаборатория Касперского», 2014. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей. Mac и Mac OS – зарегистрированные товарные знаки Apple Inc. iOS и Cisco – зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и/или ее аффилированных компаний. IBM, Lotus, Notes и Domino – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру. Linux – товарный знак Linus Torvalds, зарегистрированный в Соединенных Штатах Америки и в других странах. Microsoft, Windows, Windows Server, SharePoint, SQL Server, ActiveSync и Forefront – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах. Товарный знак BlackBerry зарегистрирован в Соединенных Штатах Америки и других странах и принадлежит Research In Motion Limited. Android – товарный знак Google, Inc. EMC и VNX – товарные знаки EMC Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

