

**Kaspersky Small Office Security**

**РУКОВОДСТВО ПО  
УСТАНОВКЕ**



**KASPERSKY** lab

# Содержание

KASPERSKY SMALL OFFICE SECURITY .....	4
Краткое описание .....	4
Комплект поставки .....	4
Начало работы .....	5
Поддержка зарегистрированных пользователей.....	7
АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ РАБОЧИХ СТАНЦИЙ WINDOWS .....	8
Получение информации о программе .....	8
Что нового в Антивирусе Касперского 6.0 для рабочих станций Windows.....	8
На чем строится защита Антивируса Касперского для рабочих станций Windows .....	9
Компоненты защиты .....	10
Задачи проверки на вирусы .....	11
Обновление.....	11
Сервисные функции программы.....	11
Установка Антивируса Касперского 6.0 для рабочих станций Windows .....	12
Аппаратные и программные требования к системе .....	13
Процедура установки с помощью мастера установки .....	13
Процедура установки программы из командной строки .....	16
Процедура установки через Редактор объектов групповой политики (Group Policy Object).....	17
Установка программы.....	17
Описание параметров файла setup.ini.....	18
Обновление версии программы .....	19
Удаление программы .....	19
Мастер первоначальной настройки .....	19
Использование объектов, сохраненных с предыдущей версии.....	19
Активация программы .....	20
Онлайн-активация .....	20
Активация пробной версии .....	21
Активация с помощью файла ключа .....	21
Завершение активации .....	21
Выбор режима защиты.....	21
Настройка параметров обновления .....	22
Настройка расписания проверки на вирусы .....	22
Ограничение доступа к программе.....	23
Настройка параметров работы Анти-Хакера.....	23
Определение статуса зоны безопасности .....	23
Формирование списка сетевых программ.....	25
Завершение работы мастера настройки.....	25
АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ СЕРВЕРОВ WINDOWS .....	26
Краткое описание.....	26
Что нового в Антивирусе Касперского 6.0 для серверов Windows .....	26
На чем строится защита Антивируса Касперского .....	27
Файловый Антивирус.....	27
Задачи проверки на вирусы .....	27

Обновление.....	28
Сервисные функции программы.....	28
Установка Антивируса Касперского 6.0 для серверов Windows.....	29
Процедура установки с помощью мастера установки.....	29
Процедура установки программы из командной строки.....	32
Процедура установки через Редактор объектов групповой политики (Group Policy Object).....	33
Установка программы.....	33
Описание параметров файла setup.ini.....	33
Обновление версии программы.....	34
Удаление программы.....	34
Мастер первоначальной настройки.....	35
Использование объектов, сохраненных с предыдущей версии.....	35
Активация программы.....	35
Онлайн-активация.....	36
Активация пробной версии.....	36
Активация с помощью файла ключа.....	36
Завершение активации.....	37
Настройка параметров обновления.....	37
Настройка расписания проверки на вирусы.....	37
Ограничение доступа к программе.....	37
Завершение работы мастера настройки.....	38
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО».....	39
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ.....	40

# KASPERSKY SMALL OFFICE SECURITY

Kaspersky Small Office Security – это программный комплекс для небольших организаций, обеспечивающий их защиту от вирусов и прочих угроз.

## КРАТКОЕ ОПИСАНИЕ

Kaspersky Small Office Security представляет собой комплект продуктов, разработанных для защиты рабочих станций и серверов под управлением Windows в локальной сети. Это Антивирус Касперского 6.0 для рабочих станций (см. Антивирус Касперского 6.0 для рабочих станций Windows, стр. [8](#)) и Антивирус Касперского 6.0 для серверов Windows (см. Антивирус Касперского 6.0 для серверов Windows, стр. [26](#)).

## КОМПЛЕКТ ПОСТАВКИ

В зависимости от размера сети, гибкая система лицензирования Kaspersky Small Office Security позволяет поддерживать следующие сочетания защищаемых компьютеров:

- 5 рабочих станций;
- 5 рабочих станций и 1 сервер;
- 10 рабочих станций и 1 сервер.

Программный продукт вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, [www.kaspersky.ru](http://www.kaspersky.ru), раздел **Интернет-магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;
- код активации приложения на футляре компакт-диска или специальном вкладыше;
- руководство пользователя;
- лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением.

При покупке Kaspersky Small Office Security в Интернет-магазине вы копируете продукт с веб-сайта Лаборатории Касперского (**Загрузить** → **Дистрибутивы продуктов**). Руководство пользователя доступно для загрузки в разделе **Загрузить** → **Документация**.

Код активации будет выслан вам электронной почтой после поступления соответствующего платежа. Установка загруженного программного обеспечения означает ваше согласие со всеми условиями лицензии.

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО "Лаборатория Касперского", в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение.

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с продуктом дистрибьютору, у которого она была приобретена, и получить назад уплаченную за нее сумму. При несогласии с

какими-либо условиями лицензионного соглашения не следует вскрывать компакт-диск, загружать, устанавливать или использовать это программное обеспечение.

## НАЧАЛО РАБОТЫ

Для установки продукта из состава Kaspersky Small Office Security на рабочую станцию или сервер, вставьте установочный компакт-диск в привод CD/DVD-ROM. Появится стартовый экран с меню диска (см. рис. 1).

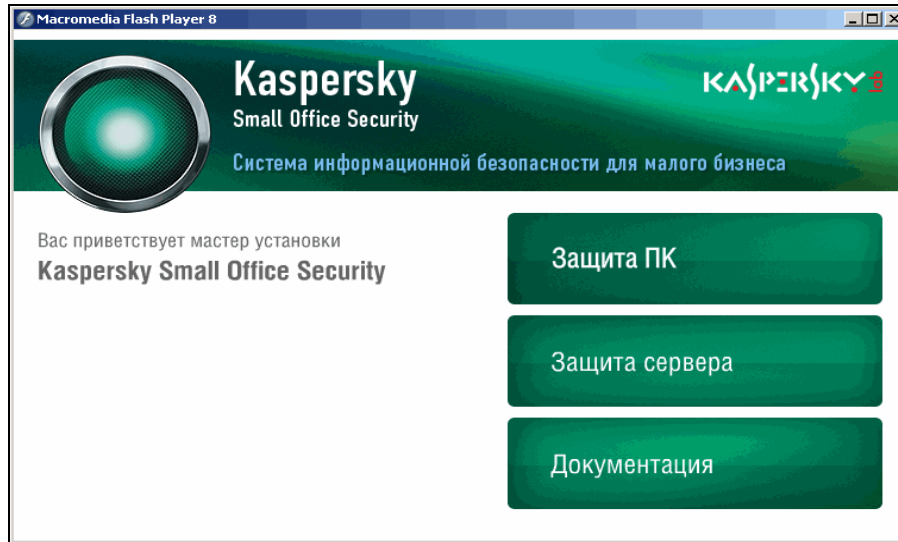


Рисунок 1. Экран автозапуска установочного диска Kaspersky Small Office Security

Выберите необходимый пункт меню:

- **Защита ПК** – для установки Антивируса Касперского на рабочую станцию. В следующем диалоге (см. рис. 2) нажмите **Установить**, чтобы запустить мастер установки, и следуйте его указаниям (см. Установка Антивируса Касперского 6.0 для рабочих станций Windows, стр. 12)

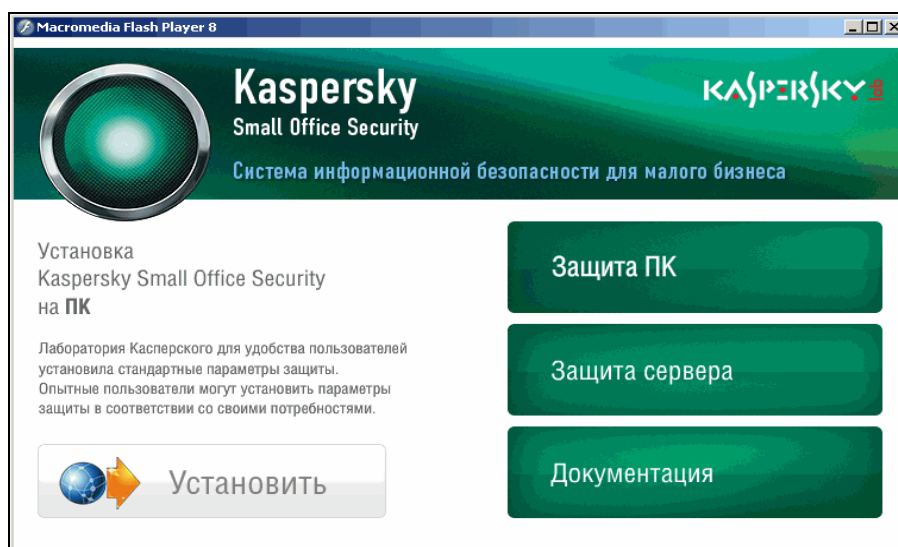


Рисунок 2. Экран автозапуска установочного диска Kaspersky Small Office Security. Установка Антивируса Касперского для рабочих станций Windows

- **Защита сервера** - для установки Антивируса Касперского на сервер. В следующем диалоге (см. рис. 3) нажмите **Установить**, чтобы запустить мастер установки, и следуйте его указаниям (см. Установка Антивируса Касперского 6.0 для серверов Windows, стр. 29).

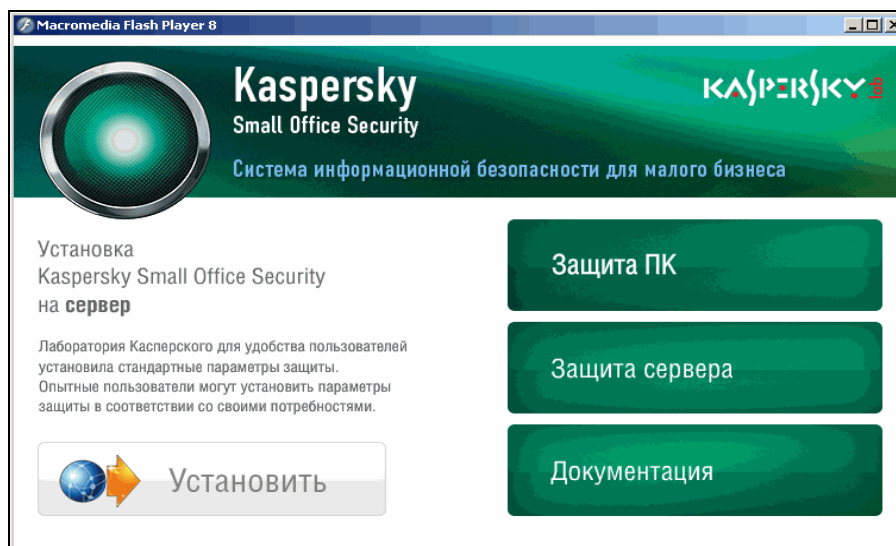


Рисунок 3. Экран автозапуска установочного диска Kaspersky Small Office Security.  
Установка Антивируса Касперского для серверов Windows

- **Документация** - для получения дополнительной информации о продуктах.

В следующем диалоге (см. рис. 4) выберите:

- **Руководство по установке Kaspersky Small Office Security**, чтобы открыть соответствующий документ.
- **Антивирус Касперского 6.0 для Windows Workstations. Руководство пользователя**, чтобы открыть соответствующий документ.
- **Антивирус Касперского 6.0 для Windows Servers. Руководство пользователя**, чтобы открыть соответствующий документ.
- **Установить Adobe Acrobat**, чтобы установить программу для просмотра документации.
- **Техническая поддержка** – для перехода на веб-сайт Службы технической поддержки Лаборатории Касперского.
- **Лаборатория Касперского** – для перехода на веб-сайт Лаборатории Касперского.



Рисунок 4. Экран автозапуска установочного диска Kaspersky Small Office Security.  
Документация

Начальный экран с меню диска отображается, только если в системе разрешен автозапуск со съемных носителей. Если эта функция отключена, следуйте инструкциям в разделе Установка Антивируса Касперского 6.0 для рабочих станций Windows, стр. [12](#), чтобы установить Антивирус Касперского для рабочих станций, и в разделе Установка Антивируса Касперского 6.0 для серверов Windows, стр. [29](#), чтобы установить Антивирус Касперского для серверов.

## ПОДДЕРЖКА ЗАРЕГИСТРИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

ЗАО "Лаборатория Касперского" предлагает своим легальным пользователям комплекс услуг, позволяющих увеличить эффективность использования Антивируса Касперского для серверов Windows.

После активации программы вы становитесь зарегистрированным пользователем и получаете возможность использовать следующие услуги в течение срока действия лицензии:

- бесплатное предоставление новых версий программы;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, предоставляемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов Лаборатории Касперского и о новых вирусах (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей Лаборатории Касперского).

Лаборатория Касперского не оказывает техническую поддержку по вопросам эксплуатации операционных систем или каких-либо продуктов сторонних разработчиков.

# АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ РАБОЧИХ СТАНЦИЙ WINDOWS

Антивирус Касперского 6.0 для рабочих станций Windows – продукт нового поколения для защиты данных.

Отличительной чертой Антивируса Касперского 6.0 для рабочих станций Windows, даже в сравнении с другими продуктами Лаборатории Касперского, является многосторонний подход к безопасности данных.

## ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ПРОГРАММЕ

Антивирус Касперского 6.0 для рабочих станций Windows – это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 6.0 для рабочих станций Windows от существующих продуктов, в том числе и от продуктов компании ЗАО «Лаборатория Касперского», – это комплексный подход к защите информации на компьютере пользователя.

## ЧТО НОВОГО В АНТИВИРУСЕ КАСПЕРСКОГО 6.0 ДЛЯ РАБОЧИХ СТАНЦИЙ WINDOWS

Антивирус Касперского 6.0 для рабочих станций Windows – это универсальное средство защиты информации. Программа обеспечивает не только антивирусную защиту, но и защиту от спама и сетевых атак. Также компоненты программы позволяют защищать компьютер от неизвестных угроз и интернет-мошенничества, контролировать доступ пользователей компьютера к интернету.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента позволяет максимально адаптировать Антивирус Касперского под нужды конкретного пользователя.

Рассмотрим детально нововведения Антивируса Касперского для рабочих станций Windows.

*Новое в защите:*

- Новое антивирусное ядро, на базе которого построен Антивирус Касперского, обладает более высокой эффективностью обнаружения вредоносных программ. Также новое антивирусное ядро обеспечивает существенное увеличение скорости проверки системы на присутствие вирусов. Это достигается за счет улучшенной обработки объектов и оптимизированного использования ресурсов компьютера (в особенности платформ на базе двух- и четырехъядерных процессоров).
- Реализован новый эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы. В случае если сигнатура программы не содержится в базах антивируса, эвристический анализатор имитирует ее запуск в изолированной виртуальной среде. Такой метод безопасен и позволяет проанализировать все действия программы еще до ее запуска в реальных условиях.
- Новый компонент Контроль доступа осуществляет контроль работы пользователя с внешними устройствами ввода / вывода, позволяя администраторам ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных.
- Значительно улучшены компоненты Сетевой экран (повышена общая эффективность компонента и добавлена поддержка протокола IPv6) и Проактивная защита (расширен список событий, обрабатываемых компонентом).

- Усовершенствована процедура обновления программы: теперь перезагрузка компьютера требуется в редких случаях.
- Добавлена проверка трафика ICQ и MSN, что обеспечивает безопасность работы с интернет-пейджерами.

#### *Новое в интерфейсе программы:*

- В интерфейсе реализован простой и удобный доступ к любому компоненту программы.
- Интерфейс разработан с учетом потребностей администраторов как небольших сетей, так и сетей крупных корпораций.

#### *Новое в работе через Kaspersky Administration Kit:*

- Kaspersky Administration Kit обеспечивает удобное и легкое управление системой антивирусной защиты организации. Программа способна осуществлять централизованное управление защитой корпоративной сети любого размера, насчитывающей десятки тысяч узлов, включая удаленных и мобильных пользователей.
- Реализована возможность удаленной установки программы с последней версией баз программы.
- Усовершенствован механизм работы с программой, установленной на удаленном компьютере (переработана структура политик).
- Добавлена возможность удаленного управления компонентами Анти-Спам и Анти-Шпион.
- Реализована возможность использования конфигурационного файла программы при создании политики.
- При настройке параметров групповых задач обновления добавлена возможность устанавливать специфические параметры для мобильных пользователей.
- Реализована возможность временно выводить клиентские компьютеры с установленной программой из области действия политик и групповых задач (после ввода установленного пароля).

## **НА ЧЕМ СТРОИТСЯ ЗАЩИТА АНТИВИРУСА КАСПЕРСКОГО ДЛЯ РАБОЧИХ СТАНЦИЙ WINDOWS**

Защита Антивируса Касперского для рабочих станций Windows строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент программы, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать программу под нужды конкретного пользователя или предприятия в целом.

Антивирус Касперского для рабочих станций Windows включает:

- Компоненты защиты (на стр. [10](#)), обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации в режиме реального времени.
- Задачи проверки на вирусы (на стр. [11](#)), посредством которых выполняется проверка компьютера или отдельных файлов, папок, дисков или областей, на присутствие вирусов.
- Обновление (на стр. [11](#)), обеспечивающее актуальность внутренних модулей программы, а также баз, используемых для поиска вредоносных программ, обнаружения хакерских атак и спам-сообщений.
- Сервисные функции (см. раздел «Сервисные функции программы» на стр. [11](#)), обеспечивающие информационную поддержку в работе с программой и позволяющие расширить ее функциональность.

## КОМПОНЕНТЫ ЗАЩИТЫ

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

### Файловый Антивирус

Файловый Антивирус контролирует файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается Антивирусом Касперского, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

### Почтовый Антивирус

Почтовый Антивирус проверяет все входящие и исходящие почтовые сообщения вашего компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов. Также компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

### Веб-Антивирус

Веб-Антивирус перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик. Также компонент анализирует веб-страницы на предмет фишинг-мошенничества.

### Проактивная защита

Проактивная защита позволяет обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. Компонент основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Антивирус Касперского принимает решение: является программа потенциально опасной или нет. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

### Анти-Шпион

Анти-Шпион отслеживает несанкционированный показ материалов рекламного характера (баннеры, всплывающие окна), перехватывает программы несанкционированного дозвона на платные интернет-ресурсы и блокирует их.

### Анти-Хакер

Анти-Хакер защищает ваш компьютер при работе в интернете и других сетях. Он контролирует исходящие и входящие соединения, проверяет порты и пакеты данных.

### Анти-Спам

Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.). Также компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

### Контроль устройств

Компонент предназначен для контроля за доступом пользователей к внешним устройствам, установленным на компьютере. Он ограничивает доступ программ к внешним устройствам (USB-, Firewire-, Bluetooth-устройства и т.д.).

## ЗАДАЧИ ПРОВЕРКИ НА ВИРУСЫ

Крайне важно периодически проводить проверку вашего компьютера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты из-за, например, установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов в состав Антивируса Касперского для рабочих станций Windows включены следующие задачи:

### Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

### Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

## ОБНОВЛЕНИЕ

Чтобы всегда быть готовым отразить любую сетевую атаку, уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского для рабочих станций Windows в актуальном состоянии. Для этого предназначен компонент **Обновление**. Он отвечает за обновление баз и модулей, используемых в работе программы.

Сервис копирования обновлений позволяет сохранять обновления баз, а также модулей программы, полученных с серверов «Лаборатории Касперского», в локальном каталоге, а затем предоставлять доступ к ним другим компьютерам сети в целях экономии интернет-трафика.

## СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ

Антивирус Касперского для рабочих станций Windows включает ряд сервисных функций. Они предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

### Файлы данных и отчеты

В процессе работы программы по каждому компоненту защиты, задаче проверки или обновлению программы формируется отчет. Он содержит информацию о выполненных операциях и результаты работы, благодаря чему вы всегда сможете узнать подробности о работе любого компонента Антивируса Касперского для рабочих станций Windows. В случае возникновения проблем отчеты можно отправлять в «Лабораторию Касперского», чтобы наши специалисты смогли подробнее изучить ситуацию и помочь вам как можно быстрее.

Все подозрительные, с точки зрения безопасности, объекты Антивируса Касперского для рабочих станций Windows переносит в специальное хранилище – *Карантин*. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Вы можете проверять эти объекты на присутствие вирусов, восстанавливать в исходном местоположении, удалять, самостоятельно добавлять объекты на карантин. Все объекты, которые по результатам проверки на вирусы окажутся незараженными, автоматически восстанавливаются в исходном местоположении.

В *Резервное хранилище* помещаются копии вылеченных и удаленных Антивирусом Касперского для рабочих станций Windows объектов. Данные копии создаются на случай необходимости восстановить объекты или

картину их заражения. Резервные копии объектов также хранятся в зашифрованном виде, чтобы избежать заражения компьютера.

Вы можете восстановить объект из резервного хранилища в исходном местоположении или удалить копию.

### Диск аварийного восстановления

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения.

### Поддержка

Все зарегистрированные пользователи Антивируса Касперского могут воспользоваться Службой технической поддержки. Для того чтобы узнать о том, где именно вы можете получить техническую поддержку, воспользуйтесь функцией **Поддержка**.

С помощью соответствующих ссылок вы можете перейти на форум пользователей продуктов «Лаборатории Касперского», а также отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе программы, заполнив специальную форму на сайте.

Также для вас доступна Служба технической поддержки онлайн, сервисы Персонального кабинета пользователя и, конечно, наши сотрудники всегда готовы вам помочь в работе с Антивирусом Касперского для рабочих станций Windows по телефону.

## УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 6.0 ДЛЯ РАБОЧИХ СТАНЦИЙ WINDOWS

Антивирус Касперского 6.0 для рабочих станций Windows может быть установлен на компьютер несколькими способами:

- локальная установка – установка программы на отдельном компьютере. Для запуска и проведения установки требуется непосредственный доступ к данному компьютеру. Локальная установка может быть проведена в одном из двух режимов:
  - интерактивном, с помощью мастера установки программы (см. раздел «Процедура установки с помощью мастера установки» на стр. [13](#)), данный режим требует участия пользователя в процессе установки;
  - неинтерактивном, запуск установки программы в данном режиме выполняется из командной строки и не требует участия пользователя в процессе установки (см. раздел «Процедура установки программы из командной строки» на стр. [16](#)).
- удаленная установка – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:
  - программного комплекса Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
  - групповых доменных политик Microsoft Windows Server 2000/2003 (см. раздел «Процедура установки через Редактор объектов групповой политики (Group Policy Object)» на стр. [17](#)).

Перед началом установки Антивируса Касперского для рабочих станций Windows (в том числе и удаленной) рекомендуется закрыть все работающие программы.

## АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ

Для нормального функционирования Антивируса Касперского 6.0 для рабочих станций Windows, компьютер должен удовлетворять следующим минимальным требованиям:

*Общие требования:*

- 300 МБ свободного места на жестком диске.
- Microsoft Internet Explorer 6.0 или выше (для обновления баз и модулей программы через интернет).
- Microsoft Windows Installer 2.0 или выше.

*Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2 или выше), Microsoft Windows XP Professional x64 (Service Pack 2 или выше):*

- Процессор Intel Pentium 300 МГц 32-bit (x86) / 64-bit (x64) или выше (или совместимый аналог).
- 256 МБ свободной оперативной памяти.

*Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1 или выше), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1 или выше), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:*

- Процессор Intel Pentium 800 МГц 32-bit (x86) / 64-bit (x64) или выше (или совместимый аналог).
- 512 МБ свободной оперативной памяти.

## ПРОЦЕДУРА УСТАНОВКИ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Чтобы установить Антивирус Касперского для рабочих станций Windows на ваш компьютер, на CD-диске с продуктом запустите файл дистрибутива.

Установка программы с дистрибутива, полученного через интернет, полностью совпадает с установкой программы с дистрибутивного CD-диска.

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Кратко поясним их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.
- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки продукта.
- **Готово** – завершить процедуру установки программы на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

### Шаг 1. Проверка соответствия системы необходимым условиям установки Антивируса Касперского для рабочих станций Windows

Перед установкой программы на компьютере выполняется проверка соответствия установленной операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского для рабочих станций Windows. Также проверяется наличие на компьютере требуемых программ и ваши права на установку программного обеспечения.

В случае если какое-либо из требований не выполнено, на экран будет выведено соответствующее уведомление. Рекомендуется установить требуемые пакеты обновлений посредством сервиса **Windows Update** и необходимые программы перед установкой Антивируса Касперского для рабочих станций Windows.

## Шаг 2. Стартовое окно процедуры установки

Если ваша система полностью соответствует предъявляемым требованиям, сразу после запуска файла дистрибутива на экране будет открыто стартовое окно, содержащее информацию о начале установки Антивируса Касперского для рабочих станций Windows на компьютер.

Для продолжения установки нажмите на кнопку **Далее**. Отказ от установки продукта выполняется по кнопке **Отмена**.

## Шаг 3. Просмотр Лицензионного соглашения

Следующее окно программы установки содержит Лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Внимательно прочтите его, и, при условии, что вы согласны со всеми пунктами соглашения, выберите вариант  **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Далее**. Установка будет продолжена.

Для отказа от установки нажмите на кнопку **Отмена**.

## Шаг 4. Выбор каталога установки

Следующий этап установки Антивируса Касперского для рабочих станций Windows определяет каталог на компьютере, в который будет установлена программа. По умолчанию задан путь:

- <Диск> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Workstations MP4 – для 32-разрядных систем.
- <Диск> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 для Windows Workstations MP4 – для 64-разрядных систем.

Вы можете указать другой каталог, нажав на кнопку **Обзор** и выбрав его в стандартном окне выбора каталога или введя путь к каталогу в соответствующем поле ввода.

Помните, если вы указываете полный путь к каталогу установки вручную, его длина не должна превышать 200 символов и содержать спецсимволы.

Для продолжения установки нажмите на кнопку **Далее**.

## Шаг 5. Использование параметров программы, сохраненных с предыдущей установки

На данном этапе вам будет предложено определить, хотите ли вы использовать в работе программой параметры защиты, базы программы и базу Анти-Спама, если таковые были сохранены на вашем компьютере при удалении предыдущей версии Антивируса Касперского 6.0 для рабочих станций Windows.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на компьютере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере базы программы, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок  **Базы программы**. Базы программы, включенные в поставку программы, не будут копироваться на компьютер.

Для того чтобы использовать параметры защиты, которые вы настроили в предыдущей версии и сохранили на компьютере, установите флажок  **Параметры работы программы**.

Также рекомендуется воспользоваться базой Анти-Спама, если таковая была сохранена при удалении предыдущей версии программы. Это позволит вам избежать процедуры обучения Анти-Спама. Чтобы учесть уже сформированную вами базу, установите флажок  **Базу Анти-Спама**.

## Шаг 6. Выбор типа установки

На данном этапе вам нужно определить полноту установки программы на ваш компьютер. Предусмотрено два варианта установки:

**Полная.** В этом случае все компоненты Антивируса Касперского для рабочих станций Windows будут установлены на ваш компьютер. Для ознакомления с дальнейшей последовательностью установки см. Шаг 8.

**Выборочная.** В данном случае вам будет предложено выбрать, какие компоненты программы вы хотите установить на ваш компьютер. Подробнее см. Шаг 7.

Для выбора типа установки нажмите на соответствующую кнопку.

## Шаг 7. Выбор компонентов программы для установки

Данный шаг выполняется только в случае **Выборочной** установки программы.

При выборочной установке вам нужно определить список компонентов Антивируса Касперского для рабочих станций Windows, которые вы хотите установить. По умолчанию для установки выбраны все компоненты защиты, компонент проверки на вирусы, а также коннектор к Агенту администрирования для удаленного управления программой через Kaspersky Administration Kit.

Для того чтобы выбрать компонент для последующей установки, нужно открыть меню по левой клавише мыши на значке рядом с именем компонента и выбрать пункт **Компонент будет установлен на локальный жесткий диск**. Подробнее о том, какую защиту обеспечивает выбранный компонент и сколько места на диске требуется для его установки, вы можете прочесть в нижней части данного окна программы установки.

Чтобы узнать подробную информацию о свободном месте на жестких дисках вашего компьютера, нажмите на кнопку **Диск**. Информация будет предоставлена в открывшемся окне.

Для отказа от установки компонента в контекстном меню выберите вариант **Компонент будет недоступен**. Помните, что, отменяя установку какого-либо компонента, вы лишаетесь защиты от целого ряда опасных программ.

После того как выбор устанавливаемых компонентов будет завершен, нажмите на кнопку **Далее**. Чтобы вернуться к списку устанавливаемых компонентов по умолчанию, нажмите на кнопку **Сброс**.

## Шаг 8. Отключение сетевого экрана Microsoft Windows

Данный шаг выполняется только в том случае, если Антивирус Касперского устанавливается на компьютер с включенным сетевым экраном, и в числе устанавливаемых компонентов присутствует Анти-Хакер.

На данном этапе установки Антивируса Касперского вам предлагается отключить сетевой экран операционной системы Microsoft Windows, поскольку входящий в состав Антивируса Касперского компонент Анти-Хакер обеспечивает полную защиту вашей работы в сети, и нет необходимости в дополнительной защите средствами операционной системы.

Если вы хотите использовать Анти-Хакер в качестве основного средства защиты при работе в сети, нажмите на кнопку **Далее**. Сетевой экран Microsoft Windows будет автоматически отключен.

Если вы хотите защищать свой компьютер с помощью сетевого экрана Microsoft Windows, выберите вариант  **Использовать сетевой экран Microsoft Windows**. В этом случае компонент Анти-Хакер будет установлен, но отключен во избежание конфликтов в работе программ.

## Шаг 9. Поиск других антивирусных программ

На этом этапе осуществляется поиск других установленных на вашем компьютере антивирусных продуктов, в том числе и продуктов «Лаборатории Касперского», совместное использование с которыми Антивируса Касперского может привести к возникновению конфликтов.

При обнаружении таких программ на вашем компьютере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Под списком обнаруженных антивирусных программ вы можете выбрать, автоматически удалить их или вручную.

Для продолжения установки нажмите на кнопку **Далее**.

## Шаг 10. Завершающая подготовка к установке программы

На данном этапе вам будет предложено произвести завершающую подготовку к установке программы на ваш компьютер.

При первоначальной установке Антивируса Касперского 6.0 для рабочих станций Windows не рекомендуется снимать флажок  **Защитить процесс установки**. Включенная защита позволит, в случае возникновения ошибок в ходе установки программы, провести корректную процедуру отката установки. При повторной попытке установки программы рекомендуется снять данный флажок.

При удаленной установке программы на компьютер через **Windows Remote Desktop** рекомендуется снимать флажок  **Защитить процесс установки**. В противном случае процедура установки может быть не проведена или проведена некорректно.

Для продолжения установки нажмите на кнопку **Установить**.

В процессе установки в составе Антивируса Касперского компонентов, перехватывающих сетевой трафик, происходит разрыв текущих сетевых соединений. Большинство прерванных соединений восстанавливается через некоторое время.

## Шаг 11. Завершение процедуры установки

Окно **Завершение установки** содержит информацию об окончании процесса установки Антивируса Касперского для рабочих станций Windows на ваш компьютер.

Для запуска мастера первоначальной настройки программы нажмите на кнопку **Далее**.

Если для корректного завершения установки необходимо перезагрузить компьютер, на экран будет выведено соответствующее уведомление.

## ПРОЦЕДУРА УСТАНОВКИ ПРОГРАММЫ ИЗ КОМАНДНОЙ СТРОКИ

- Чтобы установить Антивируса Касперского 6.0 для рабочих станций Windows, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. раздел «Процедура установки с помощью мастера установки» на стр. [13](#)). По завершении установки программы, необходимо перезагрузить компьютер.

- Чтобы установить программу в неинтерактивном режиме (без запуска мастера установки), наберите:

```
msiexec /i <имя_пакета> /qn
```

В данном случае по завершении установки программы потребуется вручную произвести перезагрузку компьютера. Для выполнения автоматической перезагрузки в командной строке наберите:

```
msiexec /i <имя_пакета> ALLOWREBOOT=1 /qn
```

Обратите внимание, что автоматическая перезагрузка компьютера может быть выполнена только в режиме неинтерактивной установки (с ключом /qn).

- *Чтобы установить программу с указанием пароля, подтверждающего право на удаление программы, наберите:*

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** – при установке программы в интерактивном режиме;
```

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** /qn – при установке программы в неинтерактивном режиме без перезагрузки компьютера;
```

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – при установке программы в неинтерактивном режиме с последующей перезагрузкой компьютера.
```

При установке Антивируса Касперского для рабочих станций Windows в неинтерактивном режиме поддерживается чтение файла `setup.ini` (см. стр. 18), содержащего общие параметры установки программы, конфигурационного файла `install.cfg`, а также файла ключа. Обратите внимание, что данные файлы должны быть расположены в одном каталоге с дистрибутивом Антивируса Касперского.

## ПРОЦЕДУРА УСТАНОВКИ ЧЕРЕЗ РЕДАКТОР ОБЪЕКТОВ ГРУППОВОЙ ПОЛИТИКИ (GROUP POLICY OBJECT)

С помощью **Редактора объектов групповой политики** вы можете устанавливать, обновлять и удалять Антивирус Касперского на рабочих станциях предприятия, входящих в состав домена, без использования Kaspersky Administration Kit.

### УСТАНОВКА ПРОГРАММЫ

- *Чтобы установить Антивирус Касперского для рабочих станций Windows, выполните следующие действия:*

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена, и поместите в нее дистрибутив Антивируса Касперского в формате `.msi`.

Дополнительно в данную директорию можно поместить файл `setup.ini` (см. стр. 18), содержащий перечень параметров установки Антивируса Касперского, конфигурационный файл `install.cfg`, а также файл ключа.

2. Откройте **Редактор объектов групповой политики** через стандартную консоль MMC (подробную информацию о работе с Редактором см. в справочной системе к Microsoft Windows Server).
3. Создайте новый пакет. Для этого в дереве консоли выберите **Объект групповой политики / Конфигурация компьютера / Конфигурация программ / Установка программного обеспечения** и воспользуйтесь командой **Создать / Пакет** контекстного меню.

В открывшемся окне укажите путь к сетевой папке общего доступа, содержащей дистрибутив Антивируса Касперского. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный** и нажмите на кнопку **ОК**.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате Антивирус Касперского для рабочих станций Windows будет установлен на все компьютеры.

## ОПИСАНИЕ ПАРАМЕТРОВ ФАЙЛА SETUP.INI

Файл *setup.ini*, расположенный в каталоге дистрибутива Антивируса Касперского, используется при установке программы в неинтерактивном режиме через командную строку или Редактор объектов групповой политики. Данный файл содержит следующие параметры:

**[Setup]** – общие параметры установки программы.

- **InstallDir**=<путь к каталогу установки программы>.
- **Reboot**=yes|no – следует ли выполнять перезагрузку компьютера по завершении установки программы (по умолчанию перезагрузка не выполняется).
- **SelfProtection**=yes|no – следует ли включать самозащиту Антивируса Касперского при установке (по умолчанию самозащита включена).
- **NoKLIM5**=yes|no – следует ли отменить установку сетевых драйверов Антивируса Касперского при установке (по умолчанию драйверы устанавливаются). Сетевые драйверы Антивируса Касперского, относящиеся к группе драйверов NDIS и отвечающие за перехват сетевого трафика для таких компонентов программы, как Анти-Хакер, Почтовый Антивирус, Веб-Антивирус и Анти-Спам, могут привести к конфликтам с другими программами или оборудованием, установленным на компьютере пользователя. На компьютерах под управлением Microsoft Windows XP или Microsoft Windows 2000 для решения возможных конфликтов можно отказаться от установки сетевых драйверов.

На компьютерах под управлением Microsoft Windows XP x64 Edition и Microsoft Vista данная возможность недоступна.

**[Components]** – выбор компонентов программы для установки. В случае если не указан ни один компонент, программа устанавливается полностью. Если указан хотя бы один из компонентов, перечисленные компоненты не устанавливаются.

- **FileMonitor**=yes|no – установка компонента Файловый Антивирус.
- **MailMonitor**=yes|no – установка компонента Почтовый Антивирус.
- **WebMonitor**=yes|no – установка компонента Веб-Антивирус.
- **ProactiveDefence**=yes|no – установка компонента Проактивная защита.
- **AntiSpy**=yes|no – установка компонента Анти-Шпион.
- **AntiHacker**=yes|no – установка компонента Анти-Хакер.
- **AntiSpam**=yes|no – установка компонента Анти-Спам.
- **LockControl**=yes|no – установка компонента Контроль устройств.

**[Tasks]** – включение задач Антивируса Касперского. В случае если не указана ни одна задача, после установки все задачи будут работать. Если указана хотя бы одна задача, все перечисленные задачи будут выключены.

- **ScanMyComputer**=yes|no – задача полной проверки.
- **ScanStartup**=yes|no – задача быстрой проверки.
- **Scan**=yes|no – задача проверки.
- **Updater**=yes|no – задача обновления баз и модулей программы.

Вместо значения **yes** могут использоваться значения 1, on, enable, enabled, а вместо значения **no** – 0, off, disable, disabled.

## ОБНОВЛЕНИЕ ВЕРСИИ ПРОГРАММЫ

➔ Для обновления версии Антивируса Касперского для рабочих станций Windows, выполните следующие действия:

1. Поместите дистрибутив, содержащий обновления Антивируса Касперского, в формате .msi в сетевую папку общего доступа.
2. Откройте **Редактор объектов групповой политики** и создайте новый пакет описанным выше способом.
3. Выберите новый пакет в списке и воспользуйтесь командой **Свойства** контекстного меню. В окне свойств пакета перейдите на закладку **Обновления** и укажите пакет, который содержит дистрибутив предыдущей версии Антивируса Касперского. Чтобы установить обновленную версию Антивируса Касперского с сохранением параметров защиты, выберите вариант установки поверх существующего пакета.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене.

## УДАЛЕНИЕ ПРОГРАММЫ

➔ Чтобы удалить Антивирус Касперского для рабочих станций Windows, выполните следующие действия:

1. Откройте **Редактор объектов групповой политики**.
2. В дереве консоли выберите **Объект\_групповой\_политики / Конфигурация компьютера/ Конфигурация программ/ Установка программного обеспечения**.

В списке пакетов выберите пакет Антивируса Касперского, откройте контекстное меню и выполните команду **Все задачи/ Удалить**.

В диалоговом окне **Удаление программ** выберите **Немедленное удаление этой программы с компьютеров всех пользователей**, чтобы Антивирус Касперского был удален при следующей перезагрузке компьютера.

## МАСТЕР ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

Мастер настройки Антивируса Касперского запускается в конце процедуры установки программы. Его задача – помочь вам провести первичную настройку параметров программы, исходя из особенностей и задач вашего компьютера.

Интерфейс мастера настройки выполнен в стиле программы-мастера для Microsoft Windows (Windows Wizard) и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Для полной установки программы на компьютер, необходимо выполнить все шаги мастера. Если по каким-либо причинам работа мастера была прервана, то уже заданные значения параметров не сохраняются. Далее, при попытке начать работу с программой, мастер первоначальной настройки запускается вновь, что влечет за собой необходимость заново производить настройку параметров.

## ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ, СОХРАНЕННЫХ С ПРЕДЫДУЩЕЙ ВЕРСИИ

Данное окно мастера появляется при установке программы поверх предыдущей версии Антивируса Касперского. Вам предлагается выбрать, какие данные, используемые предыдущей версией, требуется перенести в новую версию. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в новой версии программы, установите необходимые флажки.

## АКТИВАЦИЯ ПРОГРАММЫ

Процедура активации программы заключается в регистрации лицензии при помощи установки файла ключа. На основании лицензии программа будет определять наличие прав и срок на его использование.

Файл ключа содержит служебную информацию, необходимую для полноценной работы Антивируса Касперского, а также дополнительные сведения:

- информацию о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также дату окончания срока действия лицензии.

В зависимости от того, имеется ли у вас файл ключа или вам необходимо получить его с сервера «Лаборатории Касперского», вам предлагаются следующие варианты активации Антивируса Касперского:

- онлайн-активация (на стр. [36](#)). Выберите этот вариант активации, если вы приобрели коммерческую версию программы и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к полной функциональности программы на весь период действия лицензии.
- активация пробной версии (на стр. [36](#)). Выберите данный вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный файл ключа со сроком действия, ограниченным лицензией для пробной версии программы.
- активация с помощью полученного ранее файла ключа (см. раздел «Активация с помощью файла ключа» на стр. [36](#)). Активируйте программу с помощью полученного ранее файла ключа для Антивируса Касперского 6.0.
- активировать программу позже. При выборе этого варианта этап активации Антивируса Касперского будет пропущен. Программа будет установлена на ваш компьютер, вам будут доступны все функции программы, за исключением обновления (обновить программу вы сможете только один раз после установки). Вариант **Активировать программу позже** доступен только при первом запуске мастера активации. При последующих запусках мастера, в случае если программа уже активирована, вариант **Удалить файл ключа** для выполнения соответствующей операции.

При выборе первых двух вариантов активация программы осуществляется через веб-сервер «Лаборатории Касперского», для соединения с которым требуется подключение к интернету. Перед началом активации проверьте и, при необходимости, измените параметры сетевого соединения в окне, открываемом по кнопке **Параметры LAN**. Для получения более подробной информации о настройке сетевых параметров обратитесь к вашему системному администратору или интернет-провайдеру.

Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже из интерфейса программы либо, выйдя в интернет с другого компьютера, получить файл ключа по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

Вы также можете активировать программу через Kaspersky Administration Kit. Для этого необходимо создать задачу установки файла ключа (подробнее смотрите Справочное руководство «Kaspersky Administration Kit»).

## ОНЛАЙН-АКТИВАЦИЯ

Онлайн-активация основана на вводе кода активации, который вы получаете по электронной почте при покупке Антивируса Касперского через интернет. В случае приобретения приложения в коробке код активации будет указан на конверте с установочным диском.

## Ввод кода активации

На данном этапе требуется указать код активации. Код активации представляет собой последовательность цифр, разделенных дефисами на четыре блока по пять символов, без пробелов. Например, 11111-11111-11111-11111. Обратите внимание, что код должен вводиться латинскими символами.

В нижней части окна укажите вашу контактную информацию: фамилию, имя, отчество, адрес электронной почты, страну и город проживания. Данная информация может потребоваться для идентификации зарегистрированного пользователя, если, например, данные о лицензии были утрачены или похищены. В данном случае на основании контактных данных вы сможете получить другой код активации.

## Получение файла ключа

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете и отправляет на них ваши регистрационные данные (код активации, контактную информацию). После установления соединения на сервере проверяются код активации и полнота заполнения контактной информации. Если код активации прошел проверку, мастер получает файл ключа, который автоматически устанавливается. Процесс активации завершается, что сопровождается окном с подробной информацией о приобретенной лицензии.

Если код активации не прошел проверку, на экране появляется соответствующее уведомление. В данном случае вам следует обратиться за информацией в компанию, где вы приобрели Антивирус Касперского.

Если число активаций с помощью кода активации превышено, на экране также появляется соответствующее уведомление. Процесс активации будет прерван, и программа предложит вам обратиться в Службу поддержки «Лаборатории Касперского».

## Активация пробной версии

Данный вариант активации следует использовать, если вы хотите установить пробную версию Антивируса Касперского перед принятием решения о покупке коммерческой версии. Вам будет предоставлена бесплатная лицензия со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

## Активация с помощью файла ключа

Если у вас уже есть файл ключа, вы можете активировать Антивирус Касперского с его помощью. Для этого воспользуйтесь кнопкой **Обзор** и выберите файл с расширением `.key`.

После успешной установки ключа в нижней части окна будет представлена информация о лицензии: номер лицензии, ее тип (коммерческая, пробная и т. д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## Завершение активации

Мастер настройки информирует вас об успешном завершении активации Антивируса Касперского. Кроме того, приводится информация о лицензии: номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная и т.д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## Выбор режима защиты

В данном окне мастера настройки вам предлагается выбрать режим защиты, в котором будет работать программа:

- **Базовый.** Этот режим установлен по умолчанию и предназначен для большинства пользователей, не имеющих достаточного опыта работы с компьютером и антивирусными продуктами. Он подразумевает работу компонентов программы на рекомендуемом уровне безопасности и информирование пользователя о возникновении только опасных событий (например, обнаружение вредоносного объекта, выполнение опасных действий).

- **Интерактивный.** Этот режим предполагает расширенную защиту данных компьютера по сравнению с базовой защитой. Он позволяет отслеживать попытки изменения системных настроек, подозрительную активность в системе, а также несанкционированные действия в сети.

Все перечисленные выше действия могут являться как результатом деятельности вредоносных программ, так и быть стандартными в рамках работы программ, используемых на вашем компьютере. В каждом отдельном случае вам понадобится принять решение о допустимости или недопустимости тех или иных действий.

При выборе этого режима укажите, в каких случаях он должен использоваться:

- **Включить режим обучения Анти-Хакера** – запрашивать подтверждение действий пользователя при попытках программ, установленных на вашем компьютере, установить соединение с некоторым сетевым ресурсом. Вы можете разрешить либо запретить данное соединение, настроить правила работы Анти-Хакера для данной программы. При отключении режима обучения Антивирус Касперского работает в режиме минимальной защиты, то есть всем программам разрешен доступ к сетевым ресурсам.
- **Включить мониторинг системного реестра** – выводить запрос действий пользователя при обнаружении попыток изменения объектов системного реестра.

## НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей программы. В данном окне мастера настройки вам предлагается выбрать режим обновления программы и сформировать параметры расписания:

- **Автоматически.** Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.
- **Каждые 2 часа** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открываемом по кнопке **Изменить**.
- **Вручную.** В этом случае вы будете самостоятельно запускать обновление программы.

Обратите внимание, что базы и модули программы, входящие в дистрибутив, могут устареть на момент установки программы. Поэтому мы рекомендуем получить самые последние обновления программы. Для этого нажмите на кнопку **Обновить сейчас**. В данном случае Антивирус Касперского получит необходимый набор обновлений с сайтов обновления в интернете и установит их на компьютер.

Если вы хотите перейти к настройке параметров обновления (установить сетевые параметры, выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления от имени определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на кнопку **Настройка**.

## НАСТРОЙКА РАСПИСАНИЯ ПРОВЕРКИ НА ВИРУСЫ

Поиск вредоносных объектов в заданных областях проверки – одна из важных задач, обеспечивающих защиту компьютера.

При установке Антивируса Касперского по умолчанию создаются три задачи проверки на вирусы. В данном окне мастера настройки вам предлагается выбрать режим запуска задач проверки:

### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

## Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

## ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

В связи с тем, что персональный компьютер может использоваться несколькими людьми, в том числе с разным уровнем компьютерной грамотности, а также в связи с возможностью отключения защиты со стороны вредоносных программ, вам предлагается ограничить доступ к Антивирусу Касперского с помощью пароля. Пароль позволяет защитить программу от попыток несанкционированного отключения защиты, изменения его параметров или удаления программы.

Для включения защиты установите флажок  **Включить защиту паролем** и заполните поля **Пароль** и **Подтверждение пароля**.

Ниже укажите область, на которую будет распространяться ограничение доступа:

- **Все операции (кроме уведомлений об опасности)**. Запрашивать пароль при иницировании любого действия пользователя с программой, за исключением работы с уведомлениями об обнаружении опасных объектов.
- **Отдельные операции:**
  - **Настройка параметров программы** – запрашивать пароль при попытке пользователя изменить параметры работы Антивируса Касперского.
  - **Завершение работы программы** – запрашивать пароль при попытке пользователя завершить работу программы.
  - **Отключение компонентов защиты и остановка задач проверки** – запрашивать пароль при попытке пользователя выключить работу какого-либо компонента защиты либо остановить задачу проверки.
  - **Отключение политики Kaspersky Administration Kit** – запрашивать пароль при попытке пользователя вывести компьютер из области действия политик и групповых задач (при работе через Kaspersky Administration Kit).
  - **При удалении программы** – запрашивать пароль при попытке пользователя удалить программу с компьютера.

## НАСТРОЙКА ПАРАМЕТРОВ РАБОТЫ АНТИ-ХАКЕРА

Анти-Хакер является компонентом Антивируса Касперского, обеспечивающим безопасность работы вашего компьютера в локальных сетях и интернете. На данном этапе мастер настройки предлагает вам сформировать ряд правил, которыми Анти-Хакер будет руководствоваться при анализе сетевой активности вашего компьютера.

## ОПРЕДЕЛЕНИЕ СТАТУСА ЗОНЫ БЕЗОПАСНОСТИ

На данном этапе мастер настройки проводит анализ сетевого окружения вашего компьютера. По результатам анализа все сетевое пространство делится на условные зоны:

- *Интернет* – глобальная сеть Интернет. В данной зоне Антивирус Касперского работает как персональный сетевой экран. При этом вся сетевая активность регламентируется правилами для пакетов и программ, созданными по умолчанию для обеспечения максимальной безопасности. Вы не можете изменять условия защиты при работе в данной зоне, кроме как включить режим невидимости компьютера для дополнительной безопасности.

- **Зоны безопасности** – некоторые условные зоны, зачастую совпадающие с подсетями, в которые включен ваш компьютер (это могут быть локальные подсети дома или на работе). По умолчанию данные зоны считаются зонами средней степени риска при работе в них. Вы можете изменять статус данных зон исходя из степени доверия той или иной подсети, а также настраивать правила для пакетов и программ.

Все обнаруженные зоны представлены в списке. Для каждой из них дано описание, указаны адрес и маска подсети, а также статус, на основании которого будет разрешена либо запрещена та или иная сетевая активность в рамках работы компонента Анти-Хакер:

- **Интернет.** Этот статус по умолчанию присваивается сети Интернет, поскольку при работе в ней компьютер подвержен любым возможным типам угроз. Также данный статус рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами, фильтрами и т.д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне, а именно:
  - блокируется любая сетевая NetBios-активность в рамках подсети;
  - запрещается выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

Даже если вы создали папку общего доступа, информация, содержащаяся в ней, не будет доступна пользователям подсети с таким статусом. Кроме того, при выборе данного статуса вы не сможете получить доступ к файлам и принтерам на других компьютерах сети.

- **Локальная сеть.** Этот статус присваивается по умолчанию большинству зон безопасности, обнаруженных при анализе сетевого окружения компьютера, за исключением сети Интернет. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети). При выборе данного статуса разрешается:
  - любая сетевая NetBios-активность в рамках подсети;
  - выполнение правил для программ и пакетов, разрешающих сетевую NetBios-активность в рамках данной подсети.

Выбирайте этот статус, если вы хотите предоставить доступ к некоторым каталогам или принтерам на вашем компьютере, но запретить любую другую внешнюю активность.

- **Доверенная.** Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным. При выборе такого статуса будет разрешена любая сетевая активность. Даже если установлен уровень Максимальной защиты и созданы запрещающие правила, они не будут действовать для удаленных компьютеров доверенной зоны.

Для сети со статусом **Интернет** вы можете для дополнительной безопасности использовать *режим невидимости*. В этом режиме разрешена только сетевая активность, иницируемая с вашего компьютера. Фактически это означает, что ваш компьютер становится «невидимым» для внешнего окружения. В то же время на вашу работу в интернете режим не оказывает никакого влияния.

Не рекомендуется использовать режим невидимости, если компьютер используется в качестве сервера (например, почтового, http-сервера). Иначе, компьютеры, обращающиеся к данному серверу, не будут видеть его в сети.

Чтобы изменить статус зоны либо включить/отключить режим невидимости, выберите ее в списке и в блоке **Описание**, расположенном под списком, воспользуйтесь соответствующими ссылками. Аналогичные действия, а также редактирование адреса и маски подсети можно выполнить в окне **Параметры зоны**, открываемом по кнопке **Изменить**.

При просмотре списка зон вы можете добавить в него новую, для этого воспользуйтесь кнопкой **Найти**. Анти-Хакер произведет поиск доступных зон и, если таковые будут обнаружены, предложит вам определить их статус. Кроме того, вы можете добавить новую зону в список вручную (например, в случае, когда вы включаете мобильный компьютер в новую сеть). Для этого воспользуйтесь кнопкой **Добавить** и укажите требуемую информацию в окне **Параметры зоны**.

Чтобы удалить сеть из списка, воспользуйтесь кнопкой **Удалить**.

## **ФОРМИРОВАНИЕ СПИСКА СЕТЕВЫХ ПРОГРАММ**

Мастер настройки анализирует установленное на вашем компьютере программное обеспечение и формирует список программ, использующих для своей работы сеть.

Для каждого из таких программ Анти-Хакер создает правило, регламентирующее сетевую активность. Правила применяются на основе сформированных в «Лаборатории Касперского» и включенных в поставку продукта шаблонов наиболее распространенных программ, использующих сеть.

Список сетевых программ и правила для них вы можете посмотреть в окне настройки Анти-Хакера, которое открывается по кнопке **Список**.

В качестве дополнительной защиты рекомендуется отключить кеширование доменных имен при работе с интернет-ресурсами. Этот сервис значительно сокращает время соединения вашего компьютера с нужным интернет-ресурсом, однако в то же время является опасной уязвимостью, используя которую злоумышленники могут организовать канал утечки данных, который невозможно будет отследить с помощью сетевого экрана. Поэтому для повышения уровня безопасности вашего компьютера мы рекомендуем отключать сохранение информации о доменных именах в кеше.

## **ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА НАСТРОЙКИ**

В последнем окне мастера вам предлагается перезагрузить компьютер для завершения установки программы. Перезагрузка необходима для регистрации драйверов Антивируса Касперского для рабочих станций Windows.

Вы можете отложить перезагрузку компьютера, но в этом случае некоторые компоненты защиты программы не будут работать.

# АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ СЕРВЕРОВ WINDOWS

Антивирус Касперского 6.0 для серверов Windows – продукт нового поколения для защиты данных.

## КРАТКОЕ ОПИСАНИЕ

Антивирус Касперского для серверов Windows защищает данные, хранимые на файловых серверах под управлением Windows (включая новейшие версии x64), от всех видов вредоносных программ. Продукт обеспечивает высокую надежность и соответствует высоким требованиям к корпоративным серверам, работающим под высокой нагрузкой.

## ЧТО НОВОГО В АНТИВИРУСЕ КАСПЕРСКОГО 6.0 ДЛЯ СЕРВЕРОВ WINDOWS

Антивирус Касперского 6.0 для серверов Windows – это универсальное средство защиты информации. Рассмотрим детально нововведения Антивируса Касперского 6.0 для серверов Windows.

### *Новое в защите:*

- Новое антивирусное ядро, на базе которого построен Антивирус Касперского для серверов Windows, обладает более высокой эффективностью обнаружения вредоносных программ. Кроме того, новое антивирусное ядро обеспечивает существенное увеличение скорости проверки системы на присутствие вирусов. Это достигается за счет улучшенной обработки объектов и оптимизированного использования ресурсов компьютера (в особенности платформ на базе двух- и четырехъядерных процессоров).
- Реализован новый эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы. Если сигнатура программы не содержится в базах антивируса, эвристический анализатор имитирует ее запуск в изолированной виртуальной среде. Такой метод безопасен и позволяет проанализировать все действия программы еще до ее запуска в реальных условиях.
- Усовершенствована процедура обновления программы: теперь перезагрузка компьютера требуется в редких случаях.

### *Новое в интерфейсе программы:*

- В интерфейсе реализован простой и удобный доступ к любому компоненту программы.
- Интерфейс разработан с учетом потребностей администраторов как небольших сетей, так и сетей крупных корпораций.

### *Новое в работе через Kaspersky Administration Kit:*

- Kaspersky Administration Kit обеспечивает удобное и легкое управление системой антивирусной защиты организации. Программа способна централизованно управлять защитой корпоративной сети любого размера, насчитывающей десятки тысяч узлов, включая удаленных и мобильных пользователей.
- Реализована возможность удаленной установки программы с последней версией баз программы.
- Усовершенствован механизм работы с программой, установленной на удаленном компьютере (переработана структура политик).
- Реализована возможность использования конфигурационного файла программы при создании политики.

- При настройке параметров групповых задач обновления добавлена возможность устанавливать специфические параметры для мобильных пользователей.
- Реализована возможность временно выводить клиентские компьютеры с установленной программой из области действия политик и групповых задач (после ввода установленного пароля).

## НА ЧЕМ СТРОИТСЯ ЗАЩИТА АНТИВИРУСА КАСПЕРСКОГО

Защита включает:

- Файловый Антивирус (на стр. [27](#)), обеспечивающий контроль над объектами файловой системы компьютера в режиме реального времени.
- Задачи проверки на вирусы (на стр. [27](#)), посредством которых компьютер или отдельные файлы, папки, диски или области проверяются на присутствие вирусов.
- Обновление (на стр. [28](#)), обеспечивающее актуальность внутренних модулей программы, а также баз, используемых для поиска вредоносных программ.
- Сервисные функции (см. раздел «Сервисные функции программы» на стр. [28](#)), обеспечивающие информационную поддержку в работе с программой и позволяющие расширить ее функциональность.

### ФАЙЛОВЫЙ АНТИВИРУС

Защита сервера в реальном времени обеспечивается с помощью Файлового Антивируса.

Файловая система может содержать вирусы и другие опасные программы. Вредоносные программы могут годами храниться в вашей файловой системе, проникнув однажды со съемного диска или из интернета, и никак не проявлять себя. Однако стоит только открыть зараженный файл, вирус тут же проявит себя.

Файловый Антивирус – компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается Антивирусом Касперского, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

### ЗАДАЧИ ПРОВЕРКИ НА ВИРУСЫ

Помимо защиты с помощью Файлового Антивируса, крайне важно периодически проводить проверку сервера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены Файловым Антивирусом, например, из-за установленного низкого уровня защиты или по другим причинам.

Для проверки на вирусы в состав Антивируса Касперского включены следующие задачи:

#### Проверка

Проверка объектов, выбранных пользователем. Вы можете проверить любой объект файловой системы компьютера.

#### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.

## Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

## ОБНОВЛЕНИЕ

Чтобы всегда быть готовым уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского в актуальном состоянии. Для этого предназначен компонент **Обновление**. Он отвечает за обновление баз и модулей программы, используемых в работе программы.

Сервис копирования обновлений позволяет сохранять обновления баз, а также модулей программы, полученных с серверов «Лаборатории Касперского», в локальном каталоге, а затем предоставлять доступ к ним другим компьютерам сети в целях экономии интернет-трафика.

## СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ

Антивирус Касперского включает ряд сервисных функций. Они предусмотрены для поддержки программы в актуальном состоянии, расширения возможностей использования программы, для оказания помощи в работе.

### Файлы данных

В процессе работы программы для каждого компонента защиты, задачи проверки на вирусы или обновления программы формируется отчет. Он содержит информацию о выполненных операциях и результаты работы, благодаря чему вы всегда сможете узнать подробности о работе любого компонента Антивируса Касперского. В случае возникновения проблем отчеты можно отправлять в «Лабораторию Касперского», чтобы наши специалисты смогли подробнее изучить ситуацию и как можно быстрее вам помочь.

Все подозрительные с точки зрения безопасности объекты Антивирус Касперского переносит в специальное хранилище – *Карантин*. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Вы можете проверять эти объекты на присутствие вирусов, восстанавливать в исходном местоположении, удалять, самостоятельно добавлять объекты на карантин. Все объекты, которые по результатам проверки на вирусы окажутся незараженными, автоматически восстанавливаются в исходном местоположении.

В *Резервное хранилище* помещаются копии вылеченных и удаленных Антивирусом Касперского объектов. Данные копии создаются на случай необходимости восстановить объекты или картину их заражения. Резервные копии объектов также хранятся в зашифрованном виде, чтобы избежать заражения компьютера.

Вы можете восстановить объект из резервного хранилища в исходном местоположении или удалить копию.

### Диск восстановления

Диск аварийного восстановления предназначен для проверки и лечения зараженных x86-совместимых компьютеров. Он применяется при такой степени заражения, когда вылечить компьютер с помощью антивирусных программ или утилит лечения не представляется возможным.

### Поддержка

Все зарегистрированные пользователи Антивируса Касперского могут воспользоваться Службой технической поддержки. Чтобы узнать о том, где именно вы можете получить техническую поддержку, воспользуйтесь функцией **Поддержка**.

С помощью соответствующих ссылок можно перейти на форум пользователей продуктов «Лаборатории Касперского», просмотреть список часто задаваемых вопросов, ответы на которые, возможно, помогут в решении вашей проблемы. Кроме того, заполнив, специальную форму на сайте, вы можете отправить в Службу технической поддержки сообщение об ошибке или отзыв о работе программы.

Вам также доступна Служба технической поддержки онлайн и, конечно, наши сотрудники всегда готовы вам помочь в работе с Антивирусом Касперского по телефону.

# УСТАНОВКА АНТИВИРУСА КАСПЕРСКОГО 6.0 ДЛЯ СЕРВЕРОВ WINDOWS

Антивирус Касперского 6.0 для серверов Windows может быть установлен на компьютер несколькими способами:

- локальная установка – установка программы на отдельном компьютере. Для запуска и проведения установки требуется непосредственный доступ к данному компьютеру. Локальная установка может быть проведена в одном из двух режимов:
  - интерактивном, с помощью мастера установки программы (см. раздел «Процедура установки с помощью мастера установки» на стр. [13](#)), данный режим требует участия пользователя в процессе установки;
  - неинтерактивном, запуск установки программы в данном режиме выполняется из командной строки и не требует участия пользователя в процессе установки (см. раздел «Процедура установки программы из командной строки» на стр. [16](#)).
- удаленная установка – установка программы на компьютеры сети, выполняемая удаленно с рабочего места администратора с использованием:
  - программного комплекса Kaspersky Administration Kit (см. «Руководство по внедрению Kaspersky Administration Kit»);
  - групповых доменных политик Microsoft Windows Server 2000/2003 (см. раздел «Процедура установки через Редактор объектов групповой политики (Group Policy Object)» на стр. [17](#)).

Перед началом установки Антивируса Касперского (в том числе и удаленной) рекомендуется закрыть все работающие программы.

## ПРОЦЕДУРА УСТАНОВКИ С ПОМОЩЬЮ МАСТЕРА УСТАНОВКИ

Чтобы установить Антивирус Касперского на ваш компьютер, на CD-диске с продуктом запустите файл дистрибутива.

Установка программы с дистрибутива, полученного через интернет, полностью совпадает с установкой программы с дистрибутивного CD-диска.

Программа установки выполнена в виде мастера. Каждое окно содержит набор кнопок для управления процессом установки. Кратко поясним их назначение:

- **Далее** – принять действие и перейти к следующему шагу процедуры установки.
- **Назад** – вернуться на предыдущий шаг установки.
- **Отмена** – отказаться от установки продукта.
- **Готово** – завершить процедуру установки программы на компьютер.

Рассмотрим подробно каждый шаг процедуры установки пакета.

### Шаг 1. Проверка соответствия системы необходимым условиям установки Антивируса Касперского

Перед установкой программы на компьютере выполняется проверка соответствия установленных операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки Антивируса Касперского.

Также проверяется наличие на компьютере требуемых программ и ваши права на установку программного обеспечения.

В случае если какое-либо из требований не выполнено, на экран будет выведено соответствующее уведомление. Рекомендуется установить требуемые пакеты обновлений посредством сервиса **Windows Update** и необходимые программы перед установкой Антивируса Касперского.

## Шаг 2. Стартовое окно процедуры установки

Если ваша система полностью соответствует предъявляемым требованиям, сразу после запуска файла дистрибутива на экране будет открыто стартовое окно, содержащее информацию о начале установки Антивируса Касперского на компьютер.

Для продолжения установки нажмите на кнопку **Далее**. Отказ от установки продукта выполняется по кнопке **Отмена**.

## Шаг 3. Просмотр Лицензионного соглашения

Следующее окно программы установки содержит Лицензионное соглашение, которое заключается между вами и «Лабораторией Касперского». Внимательно прочтите его, и, при условии, что вы согласны со всеми пунктами соглашения, выберите вариант  **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Далее**. Установка будет продолжена.

Для отказа от установки нажмите на кнопку **Отмена**.

## Шаг 4. Выбор каталога установки

Следующий этап установки Антивируса Касперского определяет каталог на компьютере, в который будет установлена программа. По умолчанию задан путь:

- <Диск> → **Program Files** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 для Windows Servers MP4** – для 32-разрядных систем.
- <Диск> → **Program Files (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 для Windows Servers MP4** – для 64-разрядных систем.

Вы можете указать другой каталог, нажав на кнопку **Обзор** и выбрав его в стандартном окне выбора каталога или введя путь к каталогу в соответствующем поле ввода.

Помните, если вы указываете полный путь к каталогу установки вручную, его длина не должна превышать 200 символов и содержать спецсимволы.

Для продолжения установки нажмите на кнопку **Далее**.

## Шаг 5. Использование параметров программы, сохраненных с предыдущей установки

На данном этапе вам будет предложено определить, хотите ли вы использовать в работе программы параметры защиты и базы программы, если таковые были сохранены на сервере при удалении предыдущей версии Антивируса Касперского 6.0 для серверов Windows.

Рассмотрим подробнее, как включить использование описанных выше возможностей.

Если на компьютере ранее была установлена предыдущая версия (сборка) Антивируса Касперского, и при ее удалении вы сохранили на компьютере базы программы, вы можете подключить их для использования в устанавливаемой версии. Для этого установите флажок  **Базы программы**. Базы, включенные в поставку программы, не будут копироваться на сервер.

Для того чтобы использовать параметры защиты, которые вы настроили в предыдущей версии и сохранили на компьютере, установите флажок  **Параметры работы программы**.

## Шаг 6. Выбор типа установки

На данном этапе вам нужно определить полноту установки программы на ваш компьютер. Предусмотрено два варианта установки:

**Полная.** В этом случае все компоненты Антивируса Касперского будут установлены на сервер. Для ознакомления с дальнейшей последовательностью установки см. Шаг 8.

**Выборочная.** В данном случае вам будет предложено выбрать, какие компоненты программы вы хотите установить на сервер. Подробнее см. Шаг 7.

Для выбора типа установки нажмите на соответствующую кнопку.

## Шаг 7. Выбор компонентов программы для установки

Данный шаг выполняется только в случае **Выборочной** установки программы.

При выборочной установке вам нужно определить список компонентов Антивируса Касперского, которые вы хотите установить. По умолчанию для установки выбраны компонент Файловый Антивирус, компонент проверки на вирусы, а также коннектор к Агенту администрирования для удаленного управления программой через Kaspersky Administration Kit.

Для того чтобы выбрать компонент для последующей установки, нужно открыть меню по левой клавише мыши на значке рядом с именем компонента и выбрать пункт **Компонент будет установлен на локальный жесткий диск**. Подробнее о том, какую защиту обеспечивает выбранный компонент и сколько места на диске требуется для его установки, вы можете прочесть в нижней части данного окна программы установки.

Чтобы узнать подробную информацию о свободном месте на жестких дисках вашего компьютера, нажмите на кнопку **Диск**. Информация будет предоставлена в открывшемся окне.

Для отказа от установки компонента в контекстном меню выберите вариант **Компонент будет недоступен**. Помните, что, отменяя установку какого-либо компонента, вы лишаетесь защиты от целого ряда опасных программ.

После того как выбор устанавливаемых компонентов будет завершен, нажмите на кнопку **Далее**. Чтобы вернуться к списку устанавливаемых компонентов по умолчанию, нажмите на кнопку **Сброс**.

## Шаг 8. Поиск других антивирусных программ

На этом этапе осуществляется поиск других установленных на сервере антивирусных продуктов, в том числе и продуктов «Лаборатории Касперского», совместное использование с которыми Антивируса Касперского может привести к возникновению конфликтов.

При обнаружении таких программ на сервере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Под списком обнаруженных антивирусных программ вы можете выбрать, автоматически удалить их или вручную (автоматически будут удалены только продукты «Лаборатории Касперского»).

Для продолжения установки нажмите на кнопку **Далее**.

## Шаг 9. Завершающая подготовка к установке программы

На данном этапе вам будет предложено произвести завершающую подготовку к установке программы на сервер.

При первоначальной установке Антивируса Касперского 6.0 для серверов Windows не рекомендуется снимать флажок  **Защитить процесс установки**. Включенная защита модулей позволит, в случае возникновения ошибок в ходе установки программы, провести корректную процедуру отката установки. При повторной попытке установки программы рекомендуется снять данный флажок.

При удаленной установке программы на компьютер через **Windows Remote Desktop** рекомендуется снимать флажок  **Защитить процесс установки**. В противном случае процедура установки может быть не проведена или проведена некорректно.

Если вы хотите, чтобы в исключения автоматически были добавлены исключения, рекомендованные компанией Microsoft для серверов, установите флажок  **Исключить из антивирусной проверки области, рекомендованные компанией Microsoft**.

Если вы хотите, чтобы после установки в переменную окружения %Path% был добавлен путь к avr.com, установите флажок  **Добавить путь к avr.com к системной переменной %PATH%**.

Для продолжения установки нажмите на кнопку **Установить**.

В процессе установки в составе Антивируса Касперского компонентов, перехватывающих сетевой трафик, происходит разрыв текущих сетевых соединений. Большинство прерванных соединений восстанавливается через некоторое время.

## Шаг 10. Завершение процедуры установки

Окно **Завершение установки** содержит информацию об окончании процесса установки Антивируса Касперского на компьютер.

Для запуска мастера первоначальной настройки программы нажмите на кнопку **Далее**.

Если для корректного завершения установки необходимо перезагрузить компьютер, на экран будет выведено соответствующее уведомление.

## ПРОЦЕДУРА УСТАНОВКИ ПРОГРАММЫ ИЗ КОМАНДНОЙ СТРОКИ

➤ Чтобы установить Антивируса Касперского 6.0 для серверов Windows, наберите в командной строке:

```
msiexec /i <имя_пакета>
```

Будет запущен мастер установки (см. раздел «Процедура установки с помощью мастера установки» на стр. 13). По завершении установки программы, необходимо перезагрузить компьютер.

➤ Чтобы установить программу в неинтерактивном режиме (без запуска мастера установки), наберите:

```
msiexec /i <имя_пакета> /qn
```

В данном случае по завершении установки программы потребуется вручную произвести перезагрузку компьютера. Для выполнения автоматической перезагрузки в командной строке наберите:

```
msiexec /i <имя_пакета> ALLOWREBOOT=1 /qn
```

Обратите внимание, что автоматическая перезагрузка компьютера может быть выполнена только в режиме неинтерактивной установки (с ключом /qn).

➤ Чтобы установить программу с указанием пароля, подтверждающего право на удаление программы, наберите:

```
msiexec /i <имя_пакета> KLUNINSTPASSWD=***** – при установке программы в интерактивном режиме;
```

`msiexec /i <имя_пакета> KLUNINSTPASSWD=***** /qn` – при установке программы в неинтерактивном режиме без перезагрузки компьютера;

`msiexec /i <имя_пакета> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn` – при установке программы в неинтерактивном режиме с последующей перезагрузкой компьютера.

При установке Антивируса Касперского в неинтерактивном режиме поддерживается чтение файла `setup.ini`, содержащего общие параметры установки программы, конфигурационного файла `install.cfg`, а также файла ключа. Обратите внимание, что данные файлы должны быть расположены в одном каталоге с дистрибутивом Антивируса Касперского.

## ПРОЦЕДУРА УСТАНОВКИ ЧЕРЕЗ РЕДАКТОР ОБЪЕКТОВ ГРУППОВОЙ ПОЛИТИКИ (GROUP POLICY OBJECT)

С помощью Редактора объектов групповой политики вы можете устанавливать, обновлять и удалять Антивирус Касперского на рабочих станциях предприятия, входящих в состав домена, без использования Kaspersky Administration Kit.

### УСТАНОВКА ПРОГРАММЫ

➔ Чтобы установить Антивирус Касперского, выполните следующие действия:

1. Создайте сетевую папку общего доступа на компьютере, являющемся контроллером домена, и поместите в нее дистрибутив Антивируса Касперского в формате `.msi`.

Дополнительно в данную директорию можно поместить файл `setup.ini`, содержащий перечень параметров установки Антивируса Касперского, конфигурационный файл `install.cfg`, а также файл ключа.

2. Откройте Редактор объектов групповой политики через стандартную консоль MMC (подробную информацию о работе с Редактором см. в справочной системе к Microsoft Windows Server).
3. Создайте новый пакет. Для этого в дереве консоли выберите **Объект групповой политики / Конфигурация компьютера/ Конфигурация программ / Установка программного обеспечения** и воспользуйтесь командой **Создать / Пакет** контекстного меню.

В открывшемся окне укажите путь к сетевой папке общего доступа, содержащей дистрибутив Антивируса Касперского. В диалоговом окне **Развертывание программы** выберите параметр **Назначенный** и нажмите на кнопку **ОК**.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене. В результате Антивирус Касперского будет установлен на все компьютеры.

### ОПИСАНИЕ ПАРАМЕТРОВ ФАЙЛА SETUP.INI

Файл `setup.ini`, расположенный в каталоге дистрибутива Антивируса Касперского, используется при установке программы в неинтерактивном режиме через командную строку или Редактор объектов групповой политики. Данный файл содержит следующие параметры:

**[Setup]** – общие параметры установки программы.

- **InstallDir**=<путь к каталогу установки программы>.
- **Reboot**=yes|no – следует ли выполнять перезагрузку компьютера по завершении установки программы (по умолчанию перезагрузка не выполняется).
- **SelfProtection**=yes|no – следует ли включать самозащиту Антивируса Касперского при установке (по умолчанию самозащита включена).

- **[Components]** – выбор компонентов программы для установки. В случае если данная группа не содержит элементов, программа устанавливается полностью.
- **FileMonitor=yes|no** – установка компонента Файловый Антивирус.

**[Tasks]** – включение задач Антивируса Касперского. В случае если не указана ни одна задача, после установки все задачи будут работать. Если указана хотя бы одна задача, все перечисленные задачи будут выключены.

- **ScanMyComputer=yes|no** – задача полной проверки.
- **ScanStartup=yes|no** – задача быстрой проверки.
- **Scan=yes|no** – задача проверки.
- **Updater=yes|no** – задача обновления баз и модулей программы.

Вместо значения **yes** могут использоваться значения 1, on, enable, enabled, а вместо значения **no** – 0, off, disable, disabled.

## ОБНОВЛЕНИЕ ВЕРСИИ ПРОГРАММЫ

➔ Чтобы обновить версию Антивируса Касперского, выполните следующие действия:

1. Поместите дистрибутив, содержащий обновления Антивируса Касперского, в формате .msi в сетевую папку общего доступа.
2. Откройте **Редактор объектов групповой политики** и создайте новый пакет описанным выше способом.
3. Выберите новый пакет в списке и воспользуйтесь командой **Свойства** контекстного меню. В окне свойств пакета перейдите на закладку **Обновления** и укажите пакет, который содержит дистрибутив предыдущей версии Антивируса Касперского. Чтобы установить обновленную версию Антивируса Касперского с сохранением параметров защиты, выберите вариант установки поверх существующего пакета.

Групповая политика будет применена на каждой рабочей станции при следующей регистрации компьютеров в домене.

Обратите внимание, что на компьютерах с операционной системой Microsoft Windows 2000 Server не поддерживается обновление Антивируса Касперского через Редактор объектов групповой политики.

## УДАЛЕНИЕ ПРОГРАММЫ

➔ Чтобы удалить Антивирус Касперского, выполните следующие действия:

1. Откройте **Редактор объектов групповой политики**.
2. В дереве консоли выберите **Объект групповой политики / Конфигурация компьютера / Конфигурация программ / Установка программного обеспечения**.

В списке пакетов выберите пакет Антивируса Касперского, откройте контекстное меню и выполните команду **Все задачи / Удалить**.

В диалоговом окне **Удаление программ** выберите **Немедленное удаление этой программы с компьютеров всех пользователей**, чтобы Антивирус Касперского был удален при следующей перезагрузке компьютера.

## МАСТЕР ПЕРВОНАЧАЛЬНОЙ НАСТРОЙКИ

Мастер настройки Антивируса Касперского запускается в конце процедуры установки программы. Его задача – помочь вам провести первичную настройку параметров программы, исходя из особенностей и задач вашего компьютера.

Интерфейс мастера настройки выполнен в стиле программы-мастера для Microsoft Windows (Windows Wizard) и состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера при помощи кнопки **Готово**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Для полной установки программы на компьютер, необходимо выполнить все шаги мастера. Если по каким-либо причинам работа мастера была прервана, то уже заданные значения параметров не сохраняются. Далее, при попытке начать работу с программой, мастер первоначальной настройки запускается вновь, что влечет за собой необходимость заново производить настройку параметров.

## ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ, СОХРАНЕННЫХ С ПРЕДЫДУЩЕЙ ВЕРСИИ

Данное окно мастера появляется при установке программы поверх предыдущей версии Антивируса Касперского. Вам предлагается выбрать, какие данные, используемые предыдущей версией, требуется перенести в новую версию. Это могут быть объекты карантина, резервного хранилища либо параметры защиты.

Для того чтобы использовать эти данные в новой версии программы, установите необходимые флажки.

## АКТИВАЦИЯ ПРОГРАММЫ

Процедура активации программы заключается в регистрации лицензии при помощи установки файла ключа. На основании лицензии программа будет определять наличие прав и срок на его использование.

Файл ключа содержит служебную информацию, необходимую для полноценной работы Антивируса Касперского, а также дополнительные сведения:

- информацию о поддержке (кто осуществляет и где можно ее получить);
- название и номер ключа, а также дату окончания срока действия лицензии.

В зависимости от того, имеется ли у вас файл ключа или вам необходимо получить его с сервера «Лаборатории Каперского», вам предлагаются следующие варианты активации Антивируса Касперского:

- онлайн-активация (на стр. [36](#)). Выберите этот вариант активации, если вы приобрели коммерческую версию программы и вам был предоставлен код активации. На основании этого кода вы получите файл ключа, обеспечивающий доступ к полной функциональности программы на весь период действия лицензии.
- активация пробной версии (на стр. [36](#)). Выберите данный вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вам будет предоставлен бесплатный файл ключа со сроком действия, ограниченным лицензией для пробной версии программы.
- активация с помощью полученного ранее файла ключа (см. раздел «Активация с помощью файла ключа» на стр. [36](#)). Активируйте программу с помощью полученного ранее файла ключа для Антивируса Касперского 6.0 для серверов Windows.
- активировать программу позже. При выборе этого варианта этап активации Антивируса Касперского будет пропущен. Программа будет установлена на ваш компьютер, вам будут доступны все функции программы, за исключением обновления (обновить программу вы сможете только один раз после установки). Вариант **Активировать программу позже** доступен только при первом запуске мастера активации. При последующих запусках мастера, в случае если программа уже активирована, вариант **Удалить файл ключа** для выполнения соответствующей операции.

При выборе первых двух вариантов активация программы осуществляется через веб-сервер «Лаборатории Касперского», для соединения с которым требуется подключение к интернету. Перед началом активации проверьте и, при необходимости, измените параметры сетевого соединения в окне, открываемом по кнопке **Параметры LAN**. Для получения более подробной информации о настройке сетевых параметров обратитесь к вашему системному администратору или интернет-провайдеру.

Если на момент установки соединение с интернетом отсутствует, вы можете провести активацию позже из интерфейса программы либо, выйдя в интернет с другого компьютера, получить файл ключа по коду активации, зарегистрировавшись на веб-сайте Службы технической поддержки «Лаборатории Касперского».

Вы также можете активировать программу через Kaspersky Administration Kit. Для этого необходимо создать задачу установки файла ключа (подробнее смотрите Справочное руководство «Kaspersky Administration Kit»).

## ОНЛАЙН-АКТИВАЦИЯ

Онлайн-активация основана на вводе кода активации, который вы получаете по электронной почте при покупке Антивируса Касперского через интернет. В случае приобретения приложения в коробке код активации будет указан на конверте с установочным диском.

### Ввод кода активации

На данном этапе требуется указать код активации. Код активации представляет собой последовательность цифр, разделенных дефисами на четыре блока по пять символов, без пробелов. Например, 11111-11111-11111-11111. Обратите внимание, что код должен вводиться латинскими символами.

В нижней части окна укажите вашу контактную информацию: фамилию, имя, отчество, адрес электронной почты, страну и город проживания. Данная информация может потребоваться для идентификации зарегистрированного пользователя, если, например, данные о лицензии были утрачены или похищены. В данном случае на основании контактных данных вы сможете получить другой код активации.

### Получение файла ключа

Мастер настройки осуществляет соединение с серверами «Лаборатории Касперского» в интернете и отправляет на них ваши регистрационные данные (код активации, контактную информацию). После установления соединения на сервере проверяются код активации и полнота заполнения контактной информации. Если код активации прошел проверку, мастер получает файл ключа, который автоматически устанавливается. Процесс активации завершается, что сопровождается окном с подробной информацией о приобретенной лицензии.

Если код активации не прошел проверку, на экране появляется соответствующее уведомление. В данном случае вам следует обратиться за информацией в компанию, где вы приобрели Антивирус Касперского.

Если число активаций с помощью кода активации превышено, на экране также появляется соответствующее уведомление. Процесс активации будет прерван, и программа предложит вам обратиться в Службу поддержки «Лаборатории Касперского».

## АКТИВАЦИЯ ПРОБНОЙ ВЕРСИИ

Данный вариант активации следует использовать, если вы хотите установить пробную версию Антивируса Касперского перед принятием решения о покупке коммерческой версии. Вам будет предоставлена бесплатная лицензия со сроком действия, ограниченным лицензионным соглашением для пробной версии приложения. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

## АКТИВАЦИЯ С ПОМОЩЬЮ ФАЙЛА КЛЮЧА

Если у вас уже есть файл ключа, вы можете активировать Антивирус Касперского с его помощью. Для этого воспользуйтесь кнопкой **Обзор** и выберите файл с расширением *.key*.




После успешной установки ключа в нижней части окна будет представлена информация о лицензии: номер лицензии, ее тип (коммерческая, пробная и т. д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## ЗАВЕРШЕНИЕ АКТИВАЦИИ

Мастер настройки информирует вас об успешном завершении активации Антивируса Касперского. Кроме того, приводится информация о лицензии: номер лицензии, ее тип (коммерческая, для бета-тестирования, пробная и т.д.), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

## НАСТРОЙКА ПАРАМЕТРОВ ОБНОВЛЕНИЯ

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей программы. В данном окне мастера настройки вам предлагается выбрать режим обновления программы и сформировать параметры расписания:

-  **Автоматически.** Антивирус Касперского с заданной периодичностью проверяет наличие пакета обновлений в источнике обновления. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться вне их. При обнаружении свежих обновлений Антивирус Касперского скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.
-  **Каждые 2 часа** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открываемом по кнопке **Изменить**.
-  **Вручную.** В этом случае вы будете самостоятельно запускать обновление программы.

Обратите внимание, что базы и модули программы, входящие в дистрибутив, могут устареть на момент установки программы. Поэтому мы рекомендуем получить самые последние обновления программы. Для этого нажмите на кнопку **Обновить сейчас**. В данном случае Антивирус Касперского получит необходимый набор обновлений с сайтов обновления в интернете и установит их на компьютер.

Если вы хотите перейти к настройке параметров обновления (установить сетевые параметры, выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления от имени определенной учетной записи, а также включить сервис копирования обновлений в локальный источник), нажмите на кнопку **Настройка**.

## НАСТРОЙКА РАСПИСАНИЯ ПРОВЕРКИ НА ВИРУСЫ

Поиск вредоносных объектов в заданных областях проверки – одна из важных задач, обеспечивающих защиту компьютера.

При установке Антивируса Касперского по умолчанию создаются три задачи проверки на вирусы. В данном окне мастера настройки вам предлагается выбрать режим запуска задач проверки:

### Полная проверка

Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, исполняемые при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

### Быстрая проверка

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы. Параметры расписания можно изменить в окне, открываемом по кнопке **Изменить**.

## ОГРАНИЧЕНИЕ ДОСТУПА К ПРОГРАММЕ

Поскольку сервер могут использовать несколько человек, в том числе имеющих разные уровни компьютерной грамотности, а также в связи с тем, что вредоносные программы способны отключать защиту компьютера, вам предлагается ограничить доступ к Антивирусу Касперского с помощью пароля. Пароль позволяет защитить программу от попыток несанкционированного отключения защиты, изменения его параметров или удаления.

Для включения защиты установите флажок  **Включить защиту паролем** и заполните поля **Пароль** и **Подтверждение пароля**.

Ниже укажите область, на которую будет распространяться ограничение доступа:

- **Все операции (кроме уведомлений об опасности)**. Запрашивать пароль при инициировании любого действия пользователя с программой, за исключением работы с уведомлениями об обнаружении опасных объектов.
- **Отдельные операции:**
  - **Настройка параметров программы** – запрашивать пароль при попытке пользователя изменить параметры работы Антивируса Касперского.
  - **Завершение работы программы** – запрашивать пароль при попытке пользователя завершить работу программы.
  - **Отключение компонентов защиты и остановка задач проверки** – запрашивать пароль при попытке пользователя выключить работу Файлового Антивируса либо остановить задачу проверки на вирусы.
  - **Отключение политики Kaspersky Administration Kit** – запрашивать пароль при попытке пользователя вывести компьютер из области действия политик и групповых задач (при работе через Kaspersky Administration Kit).
  - **При удалении программы** – запрашивать пароль при попытке пользователя удалить программу с компьютера.

## ЗАВЕРШЕНИЕ РАБОТЫ МАСТЕРА НАСТРОЙКИ

В последнем окне мастера вы увидите сообщение о том, что установка и настройка Антивируса Касперского прошли успешно. Вы можете сразу запустить программу на выполнение, установив флажок  **Запустить программу**.

Если установка прошла некорректно, например, при обнаружении несовместимых версий других антивирусных программ, вам может быть предложено перезагрузить компьютер.

# ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более тысячи высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей технической поддержкой на нескольких языках.

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Веб-сайт «Лаборатории Касперского»: <http://www.kaspersky.ru>

Вирусная энциклопедия: <http://www.viruslist.ru>

Антивирусная лаборатория: [newvirus@kaspersky.com](mailto:newvirus@kaspersky.com)

(только для отправки подозрительных объектов в архивированном виде)

<http://support.kaspersky.ru/virlab/helpdesk.html>

(для запросов вирусным аналитикам)

# ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Лицензионное соглашение ЗАО «Лаборатория Касперского» с конечным пользователем о предоставлении неисключительного права на использование программного обеспечения (ПО).

**ВНИМАНИЕ!** Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.

Нажатие Вами кнопки подтверждения согласия в окне с текстом Лицензионного соглашения при установке ПО или ввод соответствующего символа(-ов) означает Ваше безоговорочное согласие с условиями настоящего Лицензионного соглашения. Если Вы не согласны с условиями настоящего Лицензионного соглашения, Вы должны прервать установку ПО.

Комплект ПО может сопровождаться дополнительным бумажным или электронным соглашением или аналогичным ему документом (далее «дополнительное соглашение»), определяющим количество компьютеров, на которых может использоваться ПО, сроки использования ПО, типы объектов, для которых предназначено ПО, и другие дополнительные условия приобретения, получения и использования ПО. В этом случае такое дополнительное соглашение является неотъемлемой частью данного Лицензионного соглашения.

## 1. Определения

1.1 **ПО** – обозначает программное обеспечение, сопроводительные материалы, обновления, описанные в Руководстве Пользователя, Правообладателем которых является ЗАО «Лаборатория Касперского».

1.2 **Правообладатель** (обладатель исключительного права на ПО) - ЗАО «Лаборатория Касперского».

1.3 **Компьютер** – оборудование, для работы на котором предназначено ПО, на которое устанавливается ПО и/или на котором используется ПО.

1.4 **Пользователь (Вы)** – физическое лицо, которое устанавливает или использует ПО от своего лица или правомочно владеет копией ПО. Если ПО было загружено или приобретено от имени юридического лица, то под термином Пользователь (Вы) далее подразумевается юридическое лицо, для которого ПО было загружено или приобретено и которое поручило отдельному физическому лицу принять данное соглашение от своего лица.

1.5 **Партнеры** – организации, осуществляющие распространение ПО на основании договора с Правообладателем.

1.6 **Обновление(-я)** – все улучшения, исправления, расширения и/или модификации ПО.

1.7 **Руководство Пользователя** – сопроводительные печатные и иные материалы, Руководство Пользователя, Руководство Администратора, справочник, файл справки и аналогичные им печатные и электронные документы, Правообладателем которых является ЗАО «Лаборатория Касперского».

1.8 **Приобретение ПО** – покупка ПО или получение ПО на условиях, изложенных в дополнительном соглашении, в том числе без выплаты вознаграждения.

## 2. Предоставление лицензии

2.1 Правообладатель предоставляет Вам неисключительную лицензию на использование ПО для защиты компьютера от угроз, описанных в Руководстве Пользователя, при условии соблюдения Вами всех технических

требований, описанных в Руководстве Пользователя, а также всех ограничений и условий использования ПО, указанных в настоящем Лицензионном соглашении.

В случае если Вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, Вы имеете право использовать ПО только в целях ознакомления и только в течение одного ознакомительного периода, если не прописано иначе, начиная с даты начальной установки ПО. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

Если Вы используете ПО разных версий ПО или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее количество Ваших компьютеров, на которых установлены и/или используются все версии ПО, должно соответствовать количеству компьютеров, указанных в лицензиях, полученных от Правообладателя *в том случае*, если условия лицензий не утверждают иное; каждая приобретенная лицензия дает Вам право установить и использовать ПО на таком количестве компьютеров, которое указано в п.2.2 и п.2.3.

2.2 В случае приобретения ПО на материальном носителе Вы имеете право использовать ПО для защиты такого количества компьютеров, которое указано на упаковке или в дополнительном соглашении.

2.3 В случае приобретения ПО через интернет Вы имеете право использовать ПО для защиты такого количества компьютеров, которое указано при оформлении покупки или в дополнительном соглашении.

2.4 Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

2.5 Вы можете передать право на использование ПО другому физическому лицу, при условии, что Вы передаете получателю право на использование ПО в пределах объема полученных прав от Правообладателя, а получатель в полном объеме соглашается с условиями настоящего Лицензионного соглашения. При передаче полного объема прав на использование ПО другому физическому лицу Вы полностью передаете получателю все полученные права на использование ПО от Правообладателя, при этом у Вас не останется ни одной копии ПО, включая архивную.

2.6 После активации ПО или выполнения процедуры установки файла ключа (за исключением ПО, предназначенного для ознакомительных целей) Вам предоставляется возможность в течение срока, указанного на упаковке (в случае приобретения ПО на материальном носителе) или указанного Вами при оформлении покупки (в случае приобретения ПО через интернет), получать от Правообладателя или его Партнеров:

- новые версии ПО по мере их выхода (через интернет);
- техническую поддержку (по телефону и/или через интернет).

### 3. Активация и сроки

3.1 Если Вы модифицируете свой компьютер или вносите изменения в программное обеспечение других правообладателей, установленное на компьютере, то может потребоваться повторная активация ПО или повторная процедура установки файла ключа. Правообладатель оставляет за собой право использовать средства для проверки наличия у Вас лицензионной копии ПО.

3.2 В случае приобретения на материальном носителе срок использования ПО указывается на упаковке или в дополнительном соглашении.

3.3 В случае приобретения ПО через интернет срок использования ПО указывается при оформлении покупки или в дополнительном соглашении.

3.4 Вы имеете право использовать ПО, предназначенное для ознакомительных целей и распространяемое без выплаты вознаграждения, как указано в п.2.1, в течение 30 (тридцати) дней с момента активации ПО в соответствии с условиями настоящего Лицензионного соглашения.

3.5 Срок полезного использования ограничивается сроком использования ПО, указанным в п.3.2 и п.3.3; информацию о сроке использования ПО можно проверить с помощью средств, указанных в Руководстве Пользователя.

3.6 В случае приобретения ПО для защиты более чем одного компьютера срок использования ПО начинается с даты активации или установки файла ключа на первом компьютере.

3.7 В случае нарушения Вами какого-либо из условий данного Лицензионного соглашения Правообладатель вправе прервать действие данного Лицензионного соглашения на использование ПО в любое время без Вашего уведомления и без возмещения стоимости ПО или его части.

#### 4. Техническая поддержка

Техническая поддержка, указанная в п. 2.6 настоящего Лицензионного соглашения, предоставляется при условии установки Пользователем последнего обновления ПО (за исключением ПО, предназначенного для ознакомительных целей).

Служба технической поддержки: <http://support.kaspersky.com>

#### 5. Предоставление информации

5.1 Для повышения уровня защиты информации Пользователя Правообладатель получает информацию об исполняемых файлах и их контрольных суммах.

5.2 В целях выявления новых угроз информационной безопасности и их источников, а также повышения уровня защиты информации пользователей ПО Правообладатель в соответствии с Положением об использовании Kaspersky Security Network получает от Пользователя информацию, определенную в Положении об использовании Kaspersky Security Network. Данную функцию автоматической передачи информации можно отключить при установке ПО, а также можно как включить, так и выключить во время работы ПО.

Полученные данные Правообладатель вправе использовать для формирования отчетов по рискам информационной безопасности.

5.3 ПО обрабатывает полученную информацию, исключая данные, относящиеся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), и никак не связывает обрабатываемую информацию с персональными данными Пользователя.

5.4 В том случае, если Вы не хотите, чтобы информация, которую Kaspersky Security Network получает от Пользователя, отсылалась Правообладателю, вы не должны активировать или должны отключить Kaspersky Security Network.

#### 6. Ограничения

- 6.1 Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством.
- 6.2 Запрещается передавать право на использование ПО третьим лицам, за исключением случаев, указанных в п.2.5 настоящего Лицензионного соглашения или в дополнительном соглашении.
- 6.3 Запрещается передавать и предоставлять доступ к коду активации и/или файлу ключа третьим лицам в нарушение положений настоящего Лицензионного соглашения, за исключением случаев, указанных в п.2.5 настоящего Лицензионного соглашения или в дополнительном соглашении. Код активации и файл ключа являются конфиденциальной информацией.
- 6.4 Запрещается сдавать ПО в аренду, прокат или во временное пользование.
- 6.5 Запрещается использовать ПО с целью создания данных или кода, предназначенных для обнаружения, блокирования или лечения угроз, описанных в Руководстве Пользователя.
- 6.6 Правообладатель имеет право заблокировать файл ключа в случае нарушения Пользователем условий настоящего Лицензионного соглашения.
- 6.7 При использовании Вами ПО, предназначенного для ознакомительных целей, Вы не имеете права получать техническую поддержку, указанную в п.4 настоящего Лицензионного соглашения, а также передавать имеющийся у Вас экземпляр ПО третьим лицам.
- 6.8 За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

## 7. Ограниченная гарантия и отказ от предоставления гарантий

- 7.1 Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Руководстве Пользователя.
- 7.2 Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.
- 7.3 Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве пользователя, а также в случае нарушения Пользователем условий настоящего Лицензионного соглашения.
- 7.4 Правообладатель не гарантирует Пользователю работоспособность ПО, если пользователь не осуществляет обновления ПО, указанных в п.2.6 настоящего Лицензионного соглашения.
- 7.5 Правообладатель не гарантирует Пользователю защиту от угроз, описанных в Руководстве Пользователя, по окончании срока, указанного в п.3.2 и п.3.3 настоящего Лицензионного соглашения.
- 7.6 ЗА ИСКЛЮЧЕНИЕМ УСТАНОВЛИВАЕМОЙ В НАСТОЯЩЕМ ПУНКТЕ ОГРАНИЧЕННОЙ ГАРАНТИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ НА ЕГО ИСПОЛЬЗОВАНИЕ ИЛИ ПРОИЗВОДИТЕЛЬНОСТЬ. ЗА ИСКЛЮЧЕНИЕМ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ, СТЕПЕНЬ КОТОРЫХ НЕ МОЖЕТ БЫТЬ ИСКЛЮЧЕНА ИЛИ ОГРАНИЧЕНА ПРИМЕНЯЕМОМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ НЕ ДАЮТ НИКАКИХ ГАРАНТИЙ, УСЛОВИЙ, ПРЕДСТАВЛЕНИЙ ИЛИ ПОЛОЖЕНИЙ (ВЫРАЖАЕМЫХ В ЯВНОЙ ИЛИ В ПОДРАЗУМЕВАЕМОЙ ФОРМЕ) НА ВСЕ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ НЕНАРУШЕНИЕ ПРАВ ТРЕТЬИХ ЛИЦ, КОММЕРЧЕСКОЕ КАЧЕСТВО, ИНТЕГРАЦИЮ ИЛИ ПРИГОДНОСТЬ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЫ СОГЛАШАЕТЕСЬ С ТЕМ, ЧТО ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ВЫБОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДОСТИЖЕНИЯ НУЖНЫХ РЕЗУЛЬТАТОВ, ЗА УСТАНОВКУ И ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ЗА РЕЗУЛЬТАТЫ, ПОЛУЧЕННЫЕ С ЕГО ПОМОЩЬЮ.

**8. Ограничение ответственности**

В МАКСИМАЛЬНОЙ СТЕПЕНИ, ДОПУСКАЕМОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, ПРАВООБЛАДАТЕЛЬ И/ИЛИ ЕГО ПАРТНЕРЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКИЕ-ЛИБО УБЫТКИ И/ИЛИ УЩЕРБ (В ТОМ ЧИСЛЕ, УБЫТКИ В СВЯЗИ С НЕДОПОЛУЧЕННОЙ КОММЕРЧЕСКОЙ ПРИБЫЛЬЮ, ПРЕРЫВАНИЕМ ДЕЯТЕЛЬНОСТИ, УТРАТОЙ ИНФОРМАЦИИ ИЛИ ИНОЙ ИМУЩЕСТВЕННОЙ УЩЕРБ), ВОЗНИКАЮЩИЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ЕСЛИ ПРАВООБЛАДАТЕЛЬ И ЕГО ПАРТНЕРЫ БЫЛИ УВЕДОМЛЕННЫ О ВОЗМОЖНОМ ВОЗНИКНОВЕНИИ ТАКИХ УБЫТКОВ И/ИЛИ УЩЕРБА. В ЛЮБОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ ПРАВООБЛАДАТЕЛЯ И ЕГО ПАРТНЕРОВ ПО ЛЮБОМУ ИЗ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ОГРАНИЧИВАЕТСЯ СУММОЙ, ФАКТИЧЕСКИ УПЛАЧЕННОЙ ВАМИ ЗА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. НАСТОЯЩИЕ ОГРАНИЧЕНИЯ НЕ МОГУТ БЫТЬ ИСКЛЮЧЕНЫ ИЛИ ОГРАНИЧЕНЫ В СООТВЕТСТВИИ С ПРИМЕНИМЫМ ПРАВОМ.

**9. Открытое (свободное) программное обеспечение**

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) Пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду («ПО с открытым исходным кодом»). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес [source@kaspersky.com](mailto:source@kaspersky.com) или сопровождается с продуктом. Если какая-либо лицензия на ПО с открытым исходным кодом требует, чтобы Правообладатель предоставлял права на использование, копирование или модификацию ПО с открытым исходным кодом, выходящие за рамки прав, предоставляемых настоящим Лицензионным соглашением, такие права имеют преимущественную силу над правами и ограничениями, оговоренными в настоящем Лицензионном соглашении.

**10. Права на интеллектуальную собственность**

10.1 Вы соглашаетесь с тем, что ПО, документация, как и все другие объекты авторского права, а также системы, идеи и методы работы, другая информация, которая содержится в ПО, товарные знаки являются объектами интеллектуальной собственности Правообладателя или его Партнеров. Данное Лицензионное соглашение не дает Вам никаких прав на использование объектов интеллектуальной собственности, включая товарные знаки и знаки обслуживания Правообладателя или его Партнеров.

10.2 Вы соглашаетесь с тем, что исходный код, код активации и/или файл ключа для ПО являются собственностью Правообладателя.

10.3 Вы соглашаетесь с тем, что не будете модифицировать или изменять ПО никаким способом. Вы не можете убирать или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

**11. Применимое законодательство**

Настоящее Лицензионное соглашение регулируется в соответствии с законодательством Российской Федерации, страны, в которой ПО используется.

## 12. Контактная информация

Центральный офис:

ЗАО «Лаборатория Касперского», 1-й Волоколамский проезд 10 корпус 1

Москва, 123060

Российская Федерация

Тел.: +7 (495) 797-8700

Факс: +7 (495) 645-7939

Адрес электронной почты: [info@kaspersky.com](mailto:info@kaspersky.com)

Веб-сайт: [www.kaspersky.com](http://www.kaspersky.com)

© ЗАО «Лаборатория Касперского», 1997-2009