

Kaspersky Security Center Web-Console



Руководство пользователя

# СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ .....	5
В этом документе.....	5
Условные обозначения.....	7
KASPERSKY SECURITY CENTER WEB-CONSOLE .....	8
ПРОГРАММНЫЕ ТРЕБОВАНИЯ .....	10
ИНТЕРФЕЙС ПРОГРАММЫ .....	11
ПОДКЛЮЧЕНИЕ К СЕРВЕРУ АДМИНИСТРИРОВАНИЯ .....	13
Подготовка к подключению к Серверу администрирования.....	13
Процесс подключения к Серверу администрирования.....	14
СОСТОЯНИЕ ЗАЩИТЫ СЕТИ.....	15
Просмотр информации о статусе компьютеров .....	15
Просмотр информации о состоянии защиты на компьютерах .....	17
Просмотр информации о состоянии баз антивирусной программы .....	19
УПРАВЛЕНИЕ КОМПЬЮТЕРАМИ.....	21
О компьютерах и группах администрирования .....	21
Просмотр списка компьютеров .....	21
Просмотр свойств компьютера .....	23
УСТАНОВКА ПРОГРАММ НА КОМПЬЮТЕРЫ СЕТИ .....	26
Об установке программ .....	26
Об агенте обновлений .....	27
Об инсталляционных пакетах .....	27
Режим удаленной установки.....	28
Назначение компьютера агентом обновлений.....	28
Удаленная установка программы .....	29
Просмотр информации о статусе удаленной установки программы .....	32
Режим локальной установки .....	33
Публикация инсталляционных пакетов .....	34
Просмотр списка опубликованных инсталляционных пакетов .....	34
Отмена публикации инсталляционного пакета .....	35
Установка программы с помощью опубликованного инсталляционного пакета .....	35
Установка программы вручную .....	36
УПРАВЛЕНИЕ ПОЛИТИКАМИ.....	37
Просмотр списка политик.....	37
Активация политики .....	38
Применение политики для автономных пользователей.....	39
Удаление политики .....	39
УПРАВЛЕНИЕ ЗАДАЧАМИ .....	40
Просмотр списка задач .....	40
Запуск и остановка задачи вручную .....	42
Просмотр результатов выполнения задачи.....	42
Удаление задачи.....	42

РАБОТА С ОТЧЕТАМИ .....	43
Об отчетах.....	43
Действия над отчетами .....	43
Просмотр отчетов .....	44
Экспорт отчета .....	45
Настройка параметров рассылки отчетов .....	45
СМЕНА ПАРОЛЯ УЧЕТНОЙ ЗАПИСИ .....	47
ВЫХОД ИЗ KASPERSKY SECURITY CENTER WEB-CONSOLE .....	48
ГЛОССАРИЙ .....	49
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» .....	51
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ .....	52
C++ JSON PARSER 4.03.....	52
FCGI-2.4.1-SNAP-0910052249 .....	52
ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE).....	53
MOD_FCGI-SNAP-0910052141.....	53
УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ .....	55
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ .....	56

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью ЗАО «Лаборатория Касперского» (далее также «Лаборатория Касперского») и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения «Лаборатории Касперского».

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу <http://www.kaspersky.ru/docs>.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, «Лаборатория Касперского» ответственности не несет.

Дата редакции документа: 12.12.2012


© ЗАО «Лаборатория Касперского», 2013

<http://www.kaspersky.ru>  
<http://support.kaspersky.ru>

# ОБ ЭТОМ РУКОВОДСТВЕ

Настоящий документ содержит информацию о программе Kaspersky Security Center Web-Console и инструкции по ее использованию.

Документ адресован техническим специалистам (администраторам) организации, в которой система безопасности на основе решений «Лаборатории Касперского» используется в качестве услуги (предоставляется поставщиком услуг защиты сети).

Если у вас возникли вопросы, связанные с использованием Kaspersky Security Center Web-Console, вы можете найти ответы на них в Руководстве пользователя и в системе встроенной справки. Справку Kaspersky Security Center Web-Console можно вызвать из главного окна программы нажатием на значок .

## В ЭТОМ РАЗДЕЛЕ

---

В этом документе .....	<a href="#">5</a>
Условные обозначения .....	<a href="#">7</a>

## В ЭТОМ ДОКУМЕНТЕ

Этот документ состоит из разделов с описанием функций и инструкциями, глоссария терминов и предметного указателя.

### **Kaspersky Security Center Web-Console (см. стр. [8](#))**

Этот раздел содержит общую информацию о программе Kaspersky Security Center Web-Console, о ее назначении и архитектуре.

### **Программные требования (см. стр. [10](#))**

Этот раздел содержит информацию о программном обеспечении, которое должно быть установлено на вашем компьютере перед тем, как вы начнете использовать программу.

### **Интерфейс программы (см. стр. [11](#))**

Этот раздел описывает назначение закладок и других элементов интерфейса, расположенных на страницах веб-портала Kaspersky Security Center Web-Console.

### **Подключение к Серверу администрирования (см. стр. [13](#))**

Этот раздел содержит инструкции о том, как подготовить подключение и подключиться к Серверу администрирования с помощью Kaspersky Security Center Web-Console.

### **Состояние защиты сети (см. стр. [15](#))**

Этот раздел содержит инструкции о том, как получить информацию о состоянии системы защиты компьютеров сети, находящихся под контролем Сервера администрирования, к которому подключена программа.

### **Управление компьютерами (см. стр. [21](#))**

Этот раздел содержит информацию о том, как просматривать списки компьютеров вашей сети и свойства компьютеров.

### **Установка программ на компьютеры сети (см. стр. [26](#))**

Этот раздел содержит инструкции о том, как устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети в режимах удаленной и локальной установки.

### **Управление политиками (см. стр. [37](#))**

Этот раздел содержит информацию об управлении политиками, сформированными для компьютеров вашей сети.

### **Управление задачами (см. стр. [40](#))**

Этот раздел содержит информацию об управлении задачами, сформированными для компьютеров вашей сети.

### **Работа с отчетами (см. стр. [43](#))**

Этот раздел содержит инструкции о том, как просматривать, распечатывать, отправлять по электронной почте отчеты Сервера администрирования, к которому подключена программа, и сохранять данные отчетов в файл.

### **Смена пароля учетной записи (см. стр. [47](#))**

Этот раздел содержит инструкцию о том, как устанавливать новый пароль для вашей учетной записи.

### **Выход из Kaspersky Security Center Web-Console (см. стр. [48](#))**

Этот раздел содержит инструкцию о том, как выйти из программы.

### **Глоссарий терминов**

Этот раздел содержит термины, используемые в документе.

### **ЗАО «Лаборатория Касперского» (см. стр. [51](#))**

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

### **Информация о стороннем коде (см. стр. [52](#))**

Этот раздел содержит информацию о стороннем коде, используемом в программе.

### **Уведомления о товарных знаках (см. стр. [55](#))**

Этот раздел содержит информацию об использованных в документе товарных знаках и их правообладателях.

### **Предметный указатель**

С помощью этого раздела вы можете быстро найти необходимые сведения в документе.

# УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В документе используются условные обозначения, описанные в таблице ниже.

Таблица 1. Условные обозначения

ПРИМЕР ТЕКСТА	ОПИСАНИЕ УСЛОВНОГО ОБОЗНАЧЕНИЯ
Обратите внимание на то, что...	Предупреждения выделяются красным цветом и заключаются в рамку. В предупреждениях содержится важная информация, например связанная с критическими для безопасности компьютера действиями.
Рекомендуется использовать...	Примечания заключаются в рамку. В примечаниях содержится вспомогательная и справочная информация.
<u>Пример:</u> ...	Примеры приводятся в блоке на желтом фоне под заголовком «Пример».
Обновление – это...	Новые термины выделяются курсивом.
ALT+F4	Названия клавиш клавиатуры выделяются полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком «плюс», означают комбинацию клавиш.
Включить	Названия элементов интерфейса, например полей ввода, команд меню, кнопок, выделяются полужирным шрифтом.
➡ Чтобы настроить расписание задачи, выполните следующие действия:	Вводные фразы инструкций выделяются курсивом.
help	Тексты командной строки или тексты сообщений, выводимых программой на экран, выделяются специальным шрифтом.
<IP-адрес вашего компьютера>	Переменные заключаются в угловые скобки. Вместо переменной в каждом случае требуется подставить соответствующее ей значение, угловые скобки при этом опускаются.

# KASPERSKY SECURITY CENTER WEB-CONSOLE

Kaspersky Security Center Web-Console представляет собой программу (веб-приложение), предназначенную для контроля состояния системы безопасности сетей организации, находящихся под защитой программ «Лаборатории Касперского».

С помощью программы вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы «Лаборатории Касперского» на компьютеры вашей сети и управлять установленными программами;
- управлять политиками и задачами, сформированными для компьютеров вашей сети;
- просматривать отчеты о состоянии системы безопасности;
- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам.

Kaspersky Security Center Web-Console работает на стороне поставщика услуг, который предоставляет услуги защиты вашей сети. Поставщик услуг защиты обеспечивает установку и обслуживание программы. Для работы с Kaspersky Security Center Web-Console вам не требуется устанавливать и запускать программу на вашем компьютере, необходимо только наличие веб-браузера (см. раздел «Программные требования» на стр. [10](#)).

Схема работы Kaspersky Security Center Web-Console представлена на рисунке ниже.

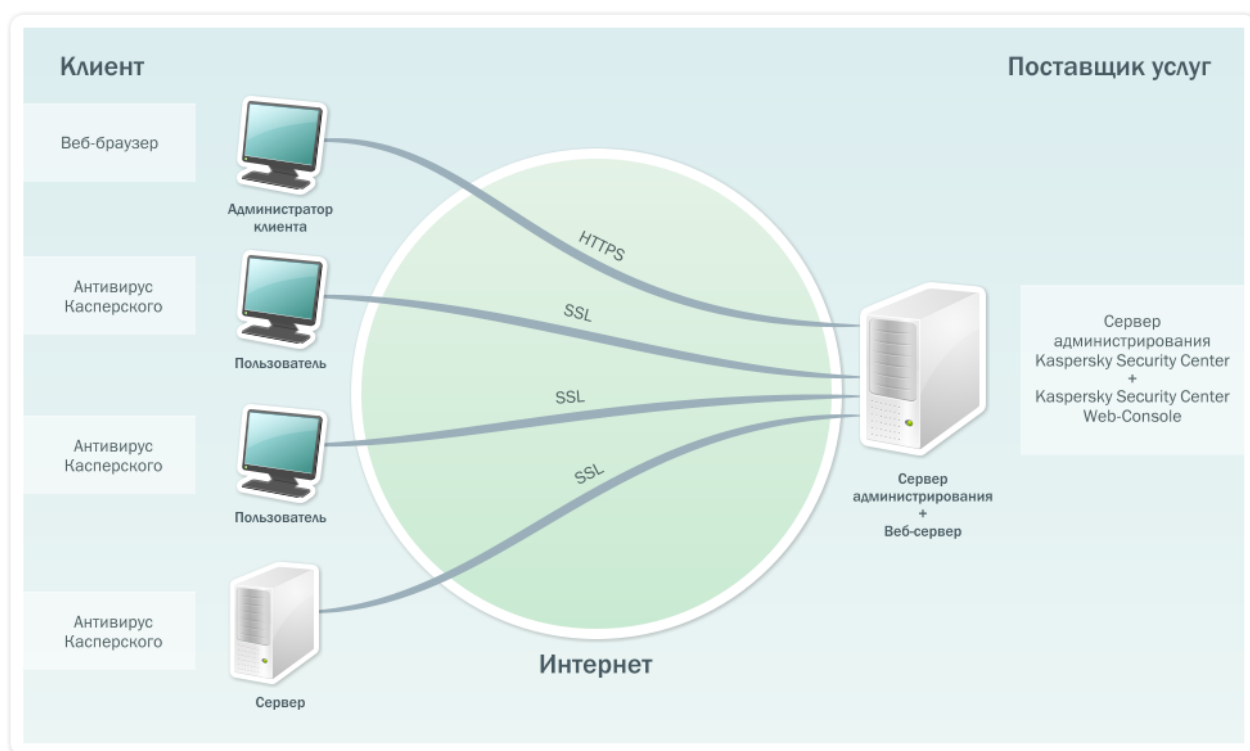


Рисунок 1. Схема работы



Kaspersky Security Center Web-Console взаимодействует с Сервером администрирования Kaspersky Security Center, который находится на стороне поставщика услуг защиты. Сервер администрирования – это программа, которая служит для управления программами «Лаборатории Касперского», установленными на компьютеры вашей сети. Сервер администрирования связывается с компьютерами вашей сети через защищенные (SSL) каналы связи.

Kaspersky Security Center Web-Console предоставляет веб-интерфейс, который обеспечивает ваше взаимодействие с Сервером администрирования с использованием веб-браузера. Когда вы с помощью вашего веб-браузера подключаетесь к Kaspersky Security Center Web-Console, веб-браузер устанавливает с Kaspersky Security Center Web-Console защищенное (HTTPS) соединение.

Kaspersky Security Center Web-Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center Web-Console с помощью веб-браузера, в окне которого отображаются страницы веб-портала программы.
2. С помощью элементов управления веб-портала вы выбираете команду, которую хотите выполнить. Kaspersky Security Center Web-Console выполняет следующие действия:
  - Если вы выбрали команду, связанную с получением информации (например, просмотр списка компьютеров), Kaspersky Security Center Web-Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их веб-браузеру в удобном для отображения виде.
  - Если вы выбрали команду управления (например, удаленная установка программы), Kaspersky Security Center Web-Console получает команду от веб-браузера и передает ее Серверу администрирования. Затем программа получает результат выполнения команды от Сервера администрирования и передает результат веб-браузеру в удобном для отображения виде.

# ПРОГРАММНЫЕ ТРЕБОВАНИЯ

В этом разделе описаны требования к программному обеспечению, необходимому для работы с Kaspersky Security Center Web-Console.

Работа с Kaspersky Security Center Web-Console осуществляется через веб-браузер. Ниже перечислены типы и версии веб-браузеров, а также типы и версии операционных систем, которые вы можете использовать для работы с программой.

- Microsoft® Internet Explorer® 7.0 или выше под управлением одной из следующих операционных систем:
  - Microsoft Windows® XP Professional с установленным Paketом обновлений 2 или выше;
  - Microsoft Windows 7;
  - Microsoft Windows 8.
- Firefox™ 16.0 и 17.0 под управлением одной из следующих операционных систем:
  - Операционные системы Windows:
    - Microsoft Windows XP Professional с установленным Paketом обновлений 2 или выше;
    - Microsoft Windows 7;
    - Microsoft Windows 8.
  - 32-битные операционные системы Linux®:
    - Fedora® 16;
    - SUSE Linux Enterprise Desktop 11 SP2;
    - Debian GNU/Linux 6.0.5;
    - Mandriva Linux 2011;
    - Ubuntu Desktop 10.04 LTS;
    - Ubuntu Server 12.04 LTS.
  - 64-битные операционные системы Linux:
    - Red Hat® Enterprise Linux 6.2 Server;
    - SUSE Linux Enterprise Desktop 11 SP2;
    - SUSE Linux Enterprise Server 11 SP2;
    - OpenSUSE Linux 12.2;
    - Ubuntu Server 12.04 LTS.
- Safari 4 под управлением одной из следующих операционных систем:
  - Mac OS X 10.4 (Tiger);
  - Mac OS X 10.5 (Leopard);
  - Mac OS X 10.6 (Snow Leopard).

# ИНТЕРФЕЙС ПРОГРАММЫ

После того как вы выполните подключение к Серверу администрирования, веб-браузер откроет главное окно Kaspersky Security Center Web-Console (см. рис. ниже).

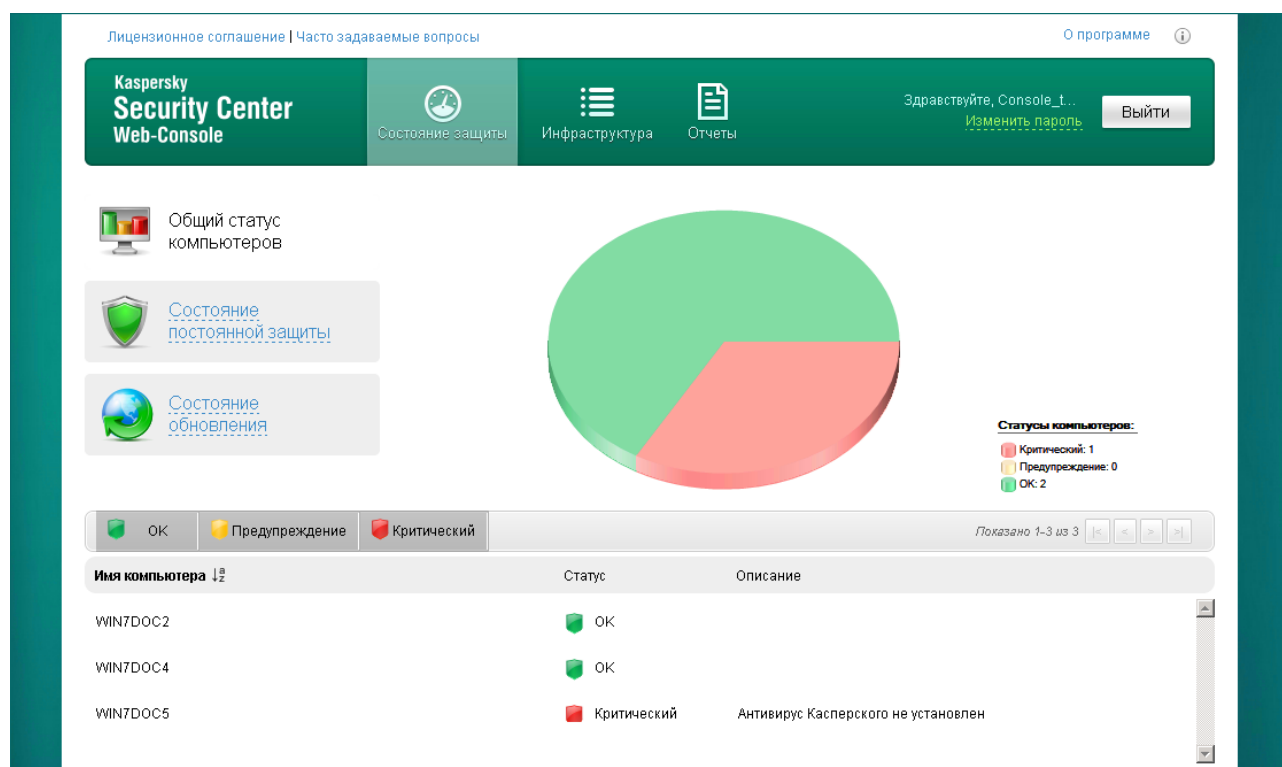


Рисунок 2. Главное окно программы

В верхней части главного окна находятся следующие элементы интерфейса:

- закладки **Состояние защиты**, **Инфраструктура** и **Отчеты** – для доступа к основным функциям программы;
- значок – для вызова контекстной справки;
- ссылка **Изменить пароль** – для смены пароля учетной записи;
- кнопка **Выход** – для завершения сеанса работы с программой;
- **Лицензионное соглашение** – ссылка на страницу с Лицензионным соглашением;
- **Часто задаваемые вопросы** – ссылка на страницу с часто задаваемыми вопросами;
- **О программе** – ссылка на страницу с информацией о программе.

Ссылки могут быть изменены администратором поставщика услуг. Некоторые ссылки могут отсутствовать.

Основное пространство главного окна занимает информационная область. Содержимое информационной области изменяется в зависимости от того, какая закладка выбрана:

- **Состояние защиты.** Содержит информацию о состоянии защиты компьютеров сети. В верхней части закладки можно выбрать один из разделов: **Общий статус**, **Состояние постоянной защиты**, **Состояние обновления**. После выбора раздела справа отображается диаграмма со статистической информацией, а в нижней части закладки отображается список с информацией о статусе компьютеров.
- **Инфраструктура.** Предназначена для получения информации о группах администрирования, компьютерах и сформированных для них политиках и задачах. Информационная область закладки разделена на две части. Левая часть информационной области содержит список групп администрирования. В правой части информационной области отображаются закладки второго уровня: **Политики**, **Задачи**, **Компьютеры**.
- **Отчеты.** Предназначена для просмотра отчетов. Информационная область закладки разделена на две части. Левая часть информационной области содержит список отчетов. В правой части информационной области отображается содержимое выбранного отчета.

## СМ. ТАКЖЕ

Подключение к Серверу администрирования.....	<a href="#">13</a>
Состояние защиты сети.....	<a href="#">15</a>
Управление компьютерами .....	<a href="#">21</a>
Работа с отчетами.....	<a href="#">43</a>
Выход из Kaspersky Security Center Web-Console.....	<a href="#">48</a>
Смена пароля учетной записи.....	<a href="#">47</a>

# ПОДКЛЮЧЕНИЕ К СЕРВЕРУ АДМИНИСТРИРОВАНИЯ

Этот раздел содержит инструкции о том, как подготовить подключение и подключиться к Серверу администрирования с помощью Kaspersky Security Center Web-Console.

## В ЭТОМ РАЗДЕЛЕ

---

Подготовка к подключению к Серверу администрирования .....	<a href="#">13</a>
Процесс подключения к Серверу администрирования .....	<a href="#">14</a>

## Подготовка к подключению к Серверу АДМИНИСТРИРОВАНИЯ

Перед подключением к Серверу администрирования вам необходимо выполнить предварительные операции: подготовить веб-браузер к работе и получить данные для подключения (адрес для подключения к Серверу администрирования и параметры учетной записи пользователя: имя пользователя и пароль).

### Подготовка веб-браузера

Перед подключением к Серверу администрирования вам необходимо убедиться, что в вашем веб-браузере включена поддержка следующих компонентов:

- JavaScript;
- файлы cookies.

Если поддержка этих компонентов отключена, вам нужно включить ее. Информацию о том как включить поддержку JavaScript и файлов cookies в вашем веб-браузере можно получить в документации к веб-браузеру.

### Получение данных для подключения

Для подключения к Серверу администрирования нужно иметь следующие данные:

- адрес веб-портала в виде `https://<Имя_домена>:<Порт>`
- имя пользователя;
- пароль.

Эту информацию вы можете получить у вашего администратора поставщика услуг.

## ПРОЦЕСС ПОДКЛЮЧЕНИЯ К СЕРВЕРУ АДМИНИСТРИРОВАНИЯ

➡ Чтобы подключиться к Серверу администрирования, выполните следующие действия:

1. Запустите веб-браузер.
2. Введите в адресной строке веб-браузера адрес веб-портала, полученный у администратора поставщика услуг (см. раздел «Подготовка к подключению к Серверу администрирования» на стр. [13](#)). Откройте этот адрес.

Если вы подключаетесь к Серверу администрирования в первый раз, в веб-браузере откроется окно **Лицензионное соглашение**. Если вы ранее подключались к Серверу администрирования, в веб-браузере откроется окно ввода имени пользователя и пароля.

3. Если вы подключаетесь к Серверу администрирования в первый раз, в окне **Лицензионное соглашение** выполните следующие действия:
  - a. Ознакомьтесь с Лицензионным соглашением. Если вы принимаете его условия, установите флажок **Принять условия Лицензионного соглашения**.
  - b. Нажмите на кнопку **Продолжить**.

В веб-браузере откроется окно ввода имени пользователя и пароля.

4. В поле **Имя пользователя** введите имя вашей учетной записи.
5. В поле **Пароль** введите пароль вашей учетной записи.
6. Введите в поле **Сервер администрирования** имя Сервера администрирования, к которому вы хотите подключиться. Нажмите на кнопку **Войти**.

Откроется главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).

Если подключение к Серверу администрирования завершилось с ошибкой, для решения проблемы обратитесь к администратору поставщика услуг.

# СОСТОЯНИЕ ЗАЩИТЫ СЕТИ

Kaspersky Security Center Web-Console позволяет получать информацию о состоянии системы защиты компьютеров сети, находящейся под контролем Сервера администрирования.

Вы можете получать следующую информацию о состоянии защиты компьютеров вашей сети:

- Общий статус компьютеров – информация о статусе компьютеров вашей сети.

Компьютер может находиться в одном из трех статусов:

- *ОК* – компьютер защищен.
- *Предупреждение* – уровень защиты компьютера снижен.
- *Критический* – уровень защиты компьютера значительно снижен.

Сервер администрирования присваивает статус компьютеру на основе информации о состоянии защиты компьютера. Статусы *Предупреждение* и *Критический* присваиваются, если существуют факторы, снижающие уровень защиты компьютера (такие как отсутствие активности антивирусной программы, устаревшие базы или большое количество невылеченных объектов). Списки этих факторов для статусов *Предупреждение* и *Критический* формирует администратор поставщика услуг.

- Состояние постоянной защиты – информация о состоянии компонента антивирусной защиты в программах «Лаборатории Касперского», установленных на компьютерах вашей сети.
- Состояние обновления – информация об актуальности баз антивирусной программы на компьютерах вашей сети.

## В ЭТОМ РАЗДЕЛЕ

Просмотр информации о статусе компьютеров.....	<a href="#">15</a>
Просмотр информации о состоянии защиты на компьютерах.....	<a href="#">17</a>
Просмотр информации о состоянии баз антивирусной программы.....	<a href="#">19</a>

## ПРОСМОТР ИНФОРМАЦИИ О СТАТУСЕ КОМПЬЮТЕРОВ

➡ Чтобы просмотреть информацию о статусе компьютеров вашей сети, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Состояние защиты**.

В главном окне программы отобразится содержимое раздела **Общий статус компьютеров** (см. рис. ниже).

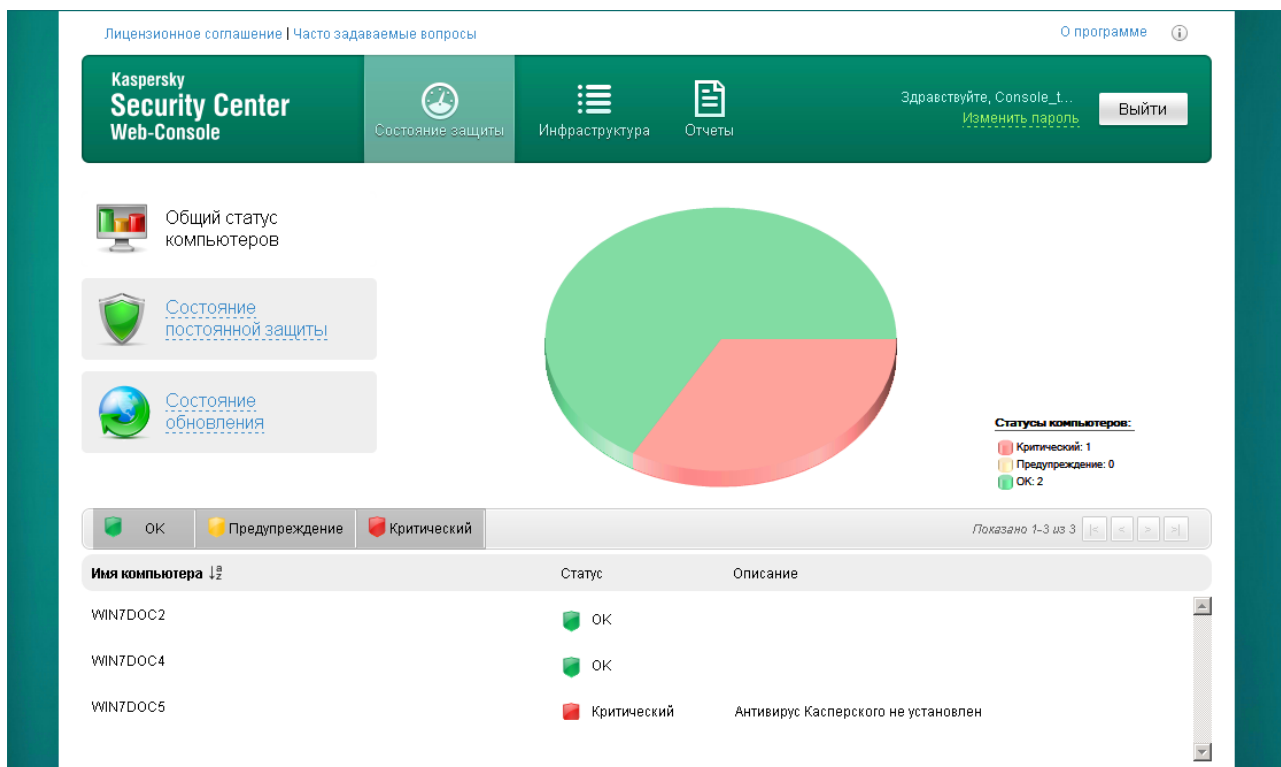


Рисунок 3. Общий статус компьютеров

В верхней части раздела расположена круговая диаграмма. Она показывает количество и процентное соотношение компьютеров со статусами *Критический*, *Предупреждение* и *ОК*.

В нижней части раздела расположен список компьютеров. Список компьютеров содержит следующую информацию о компьютерах:

- **Имя компьютера.** Имя, под которым компьютер зарегистрирован в сети.
- **Статус** (*ОК*, *Предупреждение*, *Критический*). Информация о статусе компьютера.
- **Описание.** Сообщения, описывающие причины снижения уровня безопасности компьютеров со статусами *Предупреждение* и *Критический* (такие как *Работа постоянной защиты приостановлена* или *Задача обновления не запускалась более 3-х дней*).

Чтобы просмотреть информацию о конкретном компьютере, вы можете найти его в списке компьютеров, используя следующие элементы интерфейса:

- кнопка **Критический** – отображение компьютеров со статусом *Критический*;
- кнопка **Предупреждение** – отображение компьютеров со статусом *Предупреждение*;
- кнопка **ОК** – отображение компьютеров со статусом *ОК*;
- кнопки – переход к следующей / предыдущей, первой / последней странице списка компьютеров;
- значок – сортировка имен компьютеров в списке компьютеров в алфавитном порядке по возрастанию или убыванию;
- значок – обновление списка компьютеров.

Окно с информацией о свойствах компьютера открывается нажатием клавиши мыши на строке с именем компьютера.



## СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Просмотр списка компьютеров .....	<a href="#">21</a>
Просмотр свойств компьютера .....	<a href="#">23</a>

## ПРОСМОТР ИНФОРМАЦИИ О СОСТОЯНИИ ЗАЩИТЫ НА КОМПЬЮТЕРАХ

➔ Чтобы просмотреть информацию о состоянии защиты на компьютерах вашей сети, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Состояние защиты**.
3. В левой части окна выберите раздел **Состояние постоянной защиты** (см. рис. ниже).

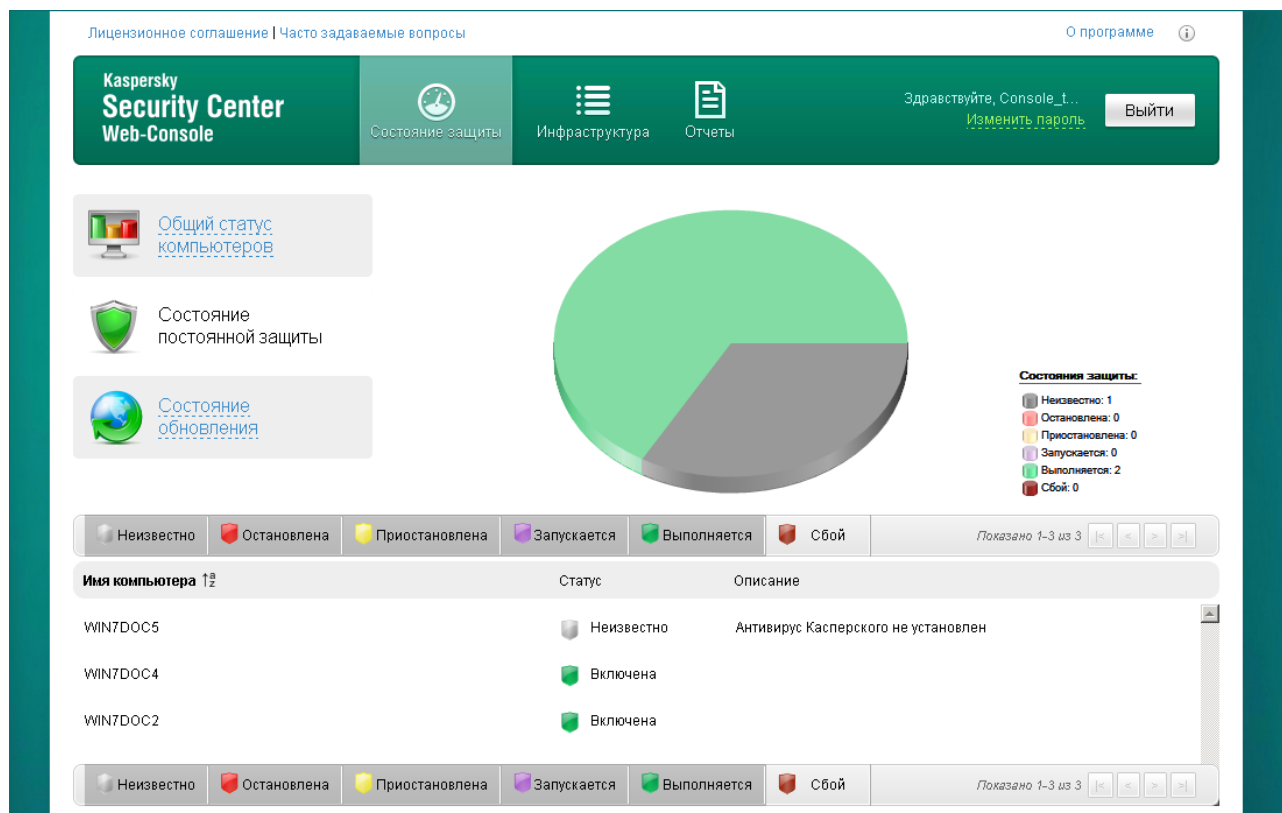


Рисунок 4. Состояние постоянной защиты

В верхней части раздела расположена круговая диаграмма. Она содержит информацию о состоянии компонента защиты в программах, установленных на компьютерах вашей сети.




Диаграмма показывает количество и процентное соотношение компьютеров, на которых компонент защиты находится в следующих состояниях:

- *Неизвестно.*
- *Остановлена.*
- *Приостановлена.*
- *Запускается.*
- *Выполняется.*
- *Сбой.*

В нижней части раздела расположен список компьютеров. Список компьютеров содержит следующую информацию о компьютерах:

- **Имя компьютера.** Имя, под которым компьютер зарегистрирован в сети.
- **Статус** (*ОК, Предупреждение, Критический*). Информация о статусе компьютера.
- **Описание.** Сообщения, описывающие причины снижения уровня безопасности компьютеров со статусами *Предупреждение* и *Критический* (такие как *Слишком большое количество невылеченных объектов* или *Срок действия лицензии истек*).

Чтобы просмотреть информацию о конкретном компьютере, вы можете найти его в списке компьютеров, используя следующие элементы интерфейса:

- кнопка **Неизвестно** – отображение компьютеров с состоянием защиты *Неизвестно*;
- кнопка **Остановлена** – отображение компьютеров с состоянием защиты *Остановлена*;
- кнопка **Приостановлена** – отображение компьютеров с состоянием защиты *Приостановлена*;
- кнопка **Запускается** – отображение компьютеров с состоянием защиты *Запускается*;
- кнопка **Выполняется** – отображение компьютеров с состоянием защиты *Выполняется*;
- кнопка **Сбой** – отображение компьютеров с состоянием защиты *Сбой*;
- кнопки  – переход к следующей / предыдущей, первой / последней странице списка компьютеров;
- значок  – сортировка имен компьютеров в списке компьютеров в алфавитном порядке по возрастанию или убыванию;
- значок  – обновление списка компьютеров.

Окно с информацией о свойствах компьютера открывается двойным щелчком мыши по строке с именем компьютера.

## СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Просмотр свойств компьютера .....	<a href="#">23</a>

## ПРОСМОТР ИНФОРМАЦИИ О СОСТОЯНИИ БАЗ АНТИВИРУСНОЙ ПРОГРАММЫ

➔ Чтобы просмотреть информацию о состоянии баз антивирусной программы на компьютерах вашей сети, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 11).
2. Выберите закладку **Состояние защиты**.
3. В левой части окна выберите раздел **Состояние обновления** (см. рис. ниже).

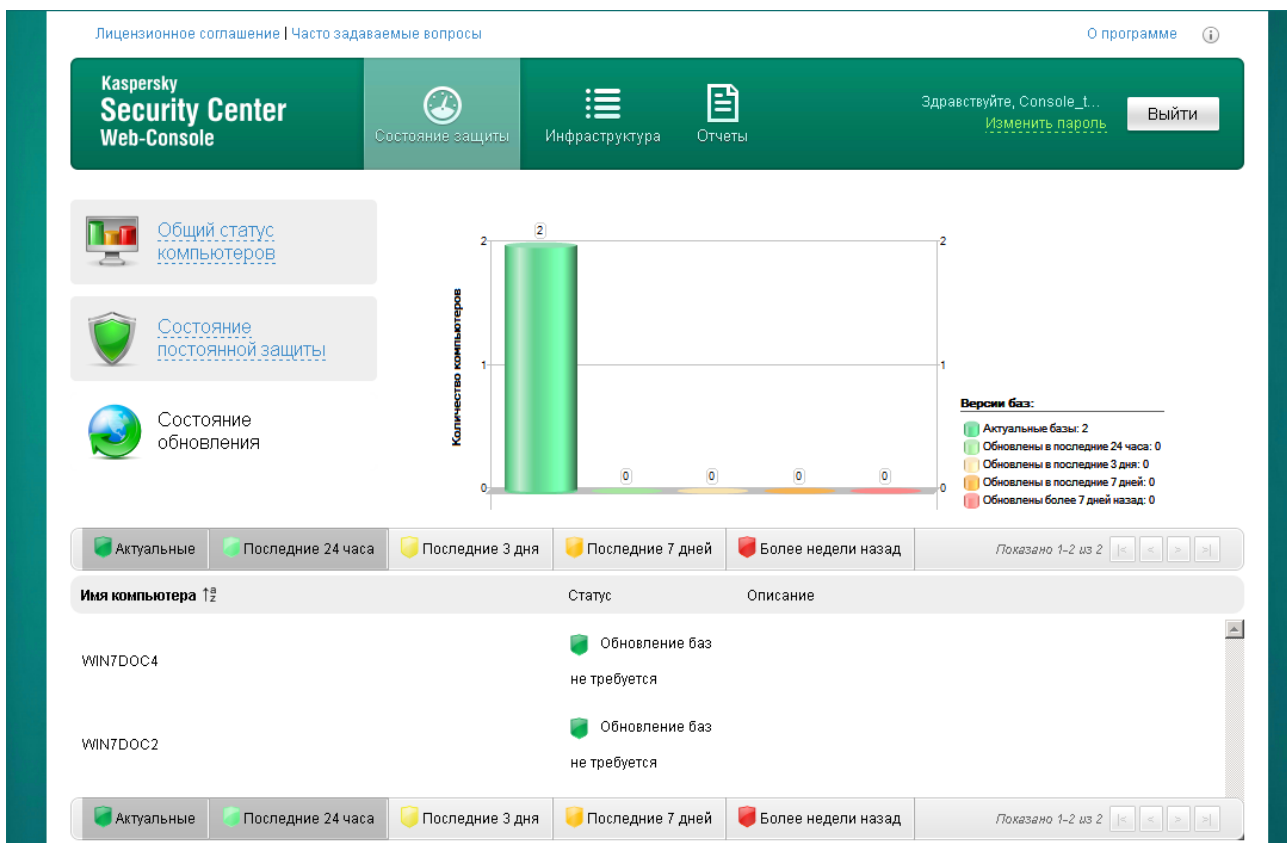


Рисунок 5. Состояние обновления

В верхней части раздела расположена столбчатая диаграмма. Она отображает информацию о состоянии баз антивирусной программы на компьютерах вашей сети.




Диаграмма показывает количество компьютеров, на которых базы антивирусной программы находятся в следующих состояниях:

- *Актуальные* – базы в актуальном состоянии.
- *Последние 24 часа* – базы обновлялись в течение последних суток.
- *Последние 3 дня* – базы обновлялись в течение последних трех дней.
- *Последние 7 дней* – базы обновлялись в течение последней недели.
- *Более недели назад* – базы обновлялись более недели назад.

В нижней части раздела расположен список компьютеров. Список компьютеров содержит следующую информацию о компьютерах:

- **Имя компьютера.** Имя, под которым компьютер зарегистрирован в сети.
- **Статус** (*ОК, Предупреждение, Критический*). Информация о статусе компьютера.
- **Описание.** Сообщения, описывающие причины снижения уровня безопасности компьютеров со статусами *Предупреждение* и *Критический* (такие как *Работа постоянной защиты приостановлена* или *Задача обновления не запускалась более 3-х дней*).

Чтобы просмотреть информацию о конкретном компьютере, вы можете найти его в списке компьютеров, используя следующие элементы интерфейса:

- кнопка **Актуальные** – отображение компьютеров, на которых базы находятся в состоянии *Актуальные*;
- кнопка **Последние 24 часа** – отображение компьютеров, на которых базы находятся в состоянии *Последние 24 часа*;
- кнопка **Последние 3 дня** – отображение компьютеров, на которых базы находятся в состоянии *Последние 3 дня*;
- кнопка **Последние 7 дней** – отображение компьютеров, на которых базы находятся в состоянии *Последние 7 дней*;
- кнопка **Более недели назад** – отображение компьютеров, на которых базы находятся в состоянии *Более недели назад*;
- кнопки  – переход к следующей / предыдущей, первой / последней странице списка компьютеров;
- значок  – сортировка имен компьютеров в списке компьютеров в алфавитном порядке по возрастанию или убыванию;
- значок  – обновление списка компьютеров.

Окно с информацией о свойствах компьютера открывается двойным щелчком мыши по строке с именем компьютера.

## СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Просмотр свойств компьютера.....	<a href="#">23</a>

# УПРАВЛЕНИЕ КОМПЬЮТЕРАМИ

Этот раздел содержит информацию о компьютерах вашей сети, о группах администрирования и инструкции о том, как просматривать списки и свойства компьютеров.

## В ЭТОМ РАЗДЕЛЕ

---

О компьютерах и группах администрирования .....	<a href="#">21</a>
Просмотр списка компьютеров .....	<a href="#">21</a>
Просмотр свойств компьютера .....	<a href="#">23</a>

## О КОМПЬЮТЕРАХ И ГРУППАХ АДМИНИСТРИРОВАНИЯ

Состояние безопасности компьютеров вашей сети контролируется Сервером администрирования поставщика услуг защиты.

Компьютеры вашей сети, на которых установлены программы «Лаборатории Касперского», распределяются по *группам администрирования*. Группы администрирования представляют собой наборы компьютеров, объединенные в соответствии с выполняемыми функциями и установленными на них программами «Лаборатории Касперского».

По умолчанию Сервер администрирования содержит группу администрирования **Управляемые**. Сервер администрирования автоматически добавляет компьютеры вашей сети в группу администрирования **Управляемые** после установки на них программ «Лаборатории Касперского». Администратор поставщика услуг может создавать другие группы администрирования и распределять по ним компьютеры. Группы администрирования могут быть созданы внутри других групп администрирования.

Компьютеры, которые включены в какую-либо группу администрирования, называются *управляемыми*. Вы можете добавлять компьютеры вашей сети в список управляемых компьютеров, в группу администрирования **Управляемые**. Для этого на компьютерах нужно установить антивирусную программу «Лаборатории Касперского».

С помощью Kaspersky Security Center Web-Console вы можете получать от Сервера администрирования информацию об управляемых компьютерах: просматривать список и свойства управляемых компьютеров.

## СМ. ТАКЖЕ

---

Установка программ на компьютеры сети .....	<a href="#">26</a>
---------------------------------------------	--------------------

## ПРОСМОТР СПИСКА КОМПЬЮТЕРОВ

Вы можете просматривать списки компьютеров вашей сети, находящихся под управлением Сервера администрирования. Вы также можете просматривать списки управляемых компьютеров отдельно в каждой из групп администрирования.

➡ Чтобы просмотреть список компьютеров, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.

3. В открывшемся окне выберите закладку **Компьютеры**.
4. В левой части окна выберите группу администрирования, список компьютеров которой вы хотите просмотреть:
  - Если вы хотите просмотреть список всех управляемых компьютеров, выберите группу **Управляемые**.
  - Если вы хотите просмотреть список управляемых компьютеров, входящих в одну из вложенных групп администрирования, выберите группу администрирования из дерева групп, расположенного под группой администрирования **Управляемые**.

На экране отобразится список компьютеров выбранной группы администрирования (см. рис. ниже).

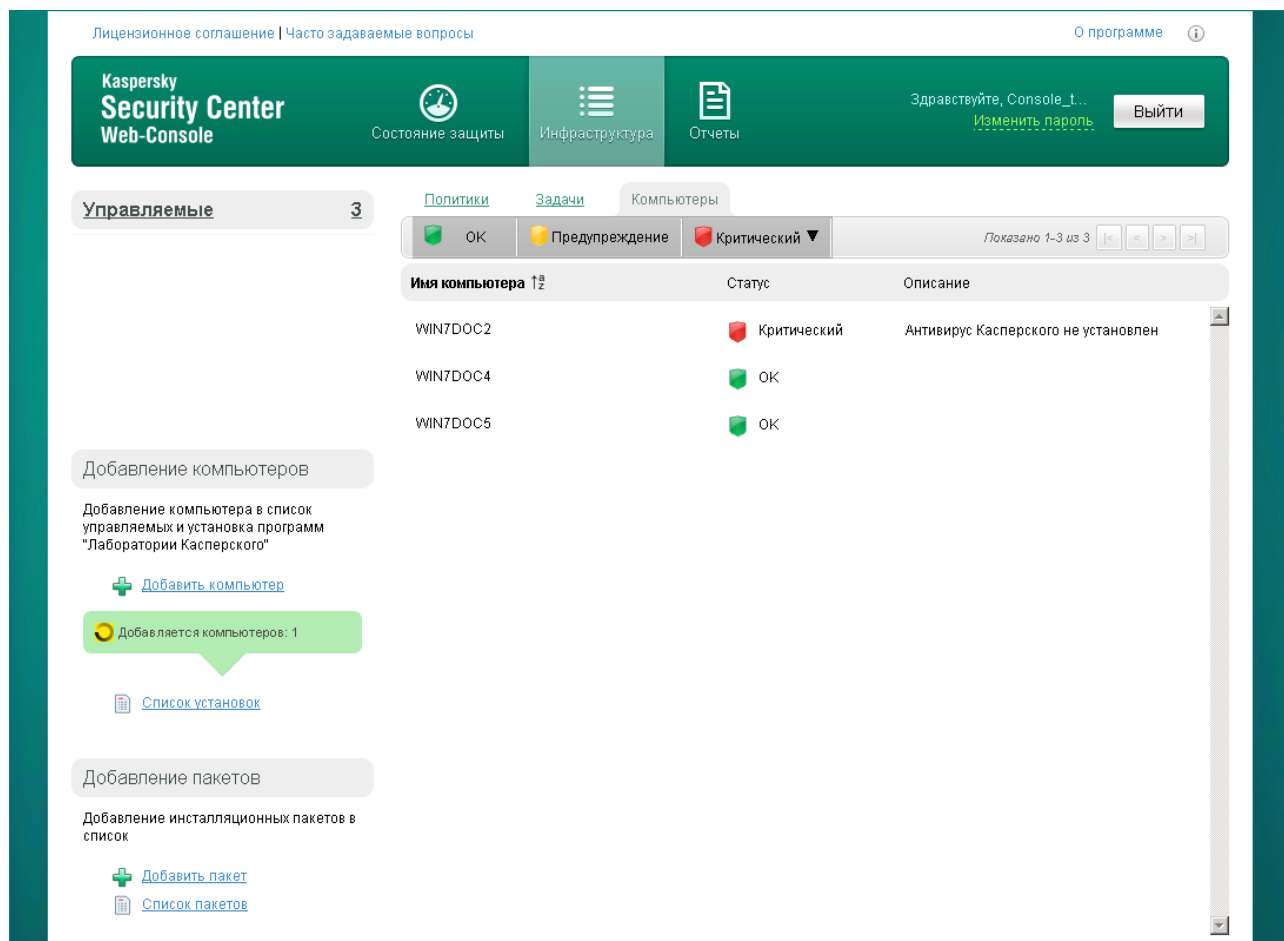





Рисунок 6. Просмотр списка компьютеров

Список компьютеров содержит следующую информацию о компьютерах:

- **Имя компьютера.** Имя, под которым компьютер зарегистрирован в сети.
- **Статус.** Статус компьютера.
- **Описание.** Сообщения, описывающие причины снижения уровня безопасности компьютеров со статусами *Предупреждение* и *Критический* (например, такие как *Работа постоянной защиты приостановлена* или *Задача обновления не запускалась более 3-х дней*).

Чтобы просмотреть информацию о конкретном компьютере, вы можете найти его в списке компьютеров, используя следующие элементы интерфейса:

- кнопка **Критический** – отображение компьютеров со статусом *Критический*;
- кнопка **Предупреждение** – отображение компьютеров со статусом *Предупреждение*;
- кнопка **ОК** – отображение компьютеров со статусом *ОК*;
- кнопки  – переход к следующей / предыдущей, первой / последней странице списка компьютеров;
- значок  – сортировка имен компьютеров в списке компьютеров в алфавитном порядке по возрастанию или убыванию;
- значок  – обновление списка компьютеров.

Окно с информацией о свойствах компьютера открывается нажатием клавиши мыши на строке с именем компьютера.

### СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Состояние защиты сети .....	<a href="#">15</a>

## ПРОСМОТР СВОЙСТВ КОМПЬЮТЕРА

➡ Чтобы просмотреть свойства компьютера, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Компьютеры**.

3. Выберите в списке групп администрирования в левой части окна группу администрирования, где находится необходимый вам компьютер.

В правой части окна отобразится список компьютеров выбранной группы администрирования.

4. Выберите в списке компьютер, свойства которого вы хотите просмотреть, и нажатием клавиши мыши на строке с именем компьютера откройте окно с информацией о свойствах компьютера (см. рис. ниже).

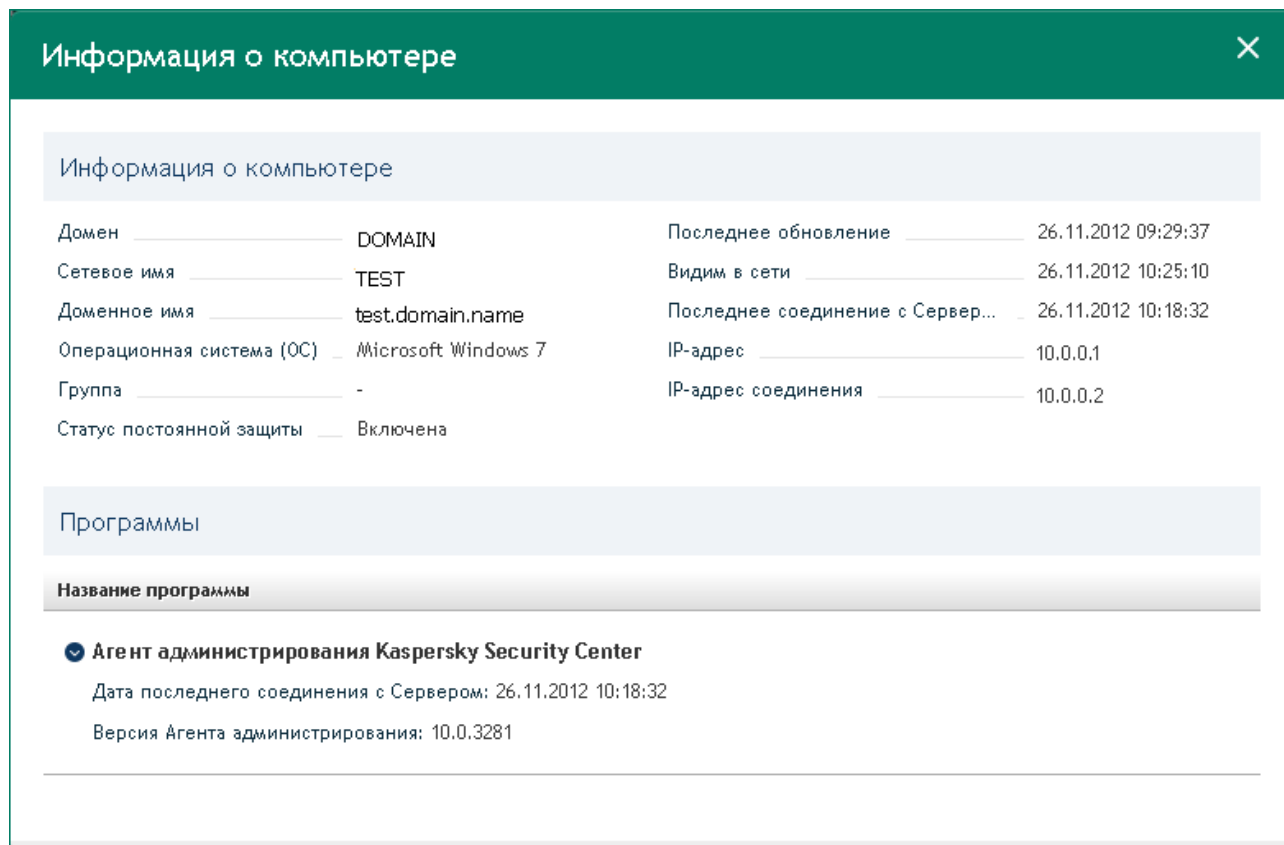


Рисунок 7. Просмотр свойств компьютера

Окно со свойствами компьютера разделено на две части.

Верхняя часть окна содержит информацию о следующих свойствах компьютера:

- **Домен.** Имя сетевого домена, в котором зарегистрирован компьютер.
- **Сетевое имя.** Имя, под которым компьютер зарегистрирован в сети. Совпадает с именем компьютера, которое отображается в левой части окна.
- **Доменное имя.** Полное доменное имя компьютера в виде <Имя\_компьютера>.<Имя\_домена>.
- **Операционная система (ОС).** Тип операционной системы, которая установлена на компьютере.
- **Группа.** Имя группы администрирования, в которую включен компьютер.
- **Статус постоянной защиты.** Состояние постоянной защиты компьютера.
- **Последнее обновление.** Дата последнего обновления программ или антивирусных баз «Лаборатории Касперского» на компьютере.
- **Видим в сети.** Дата и время, начиная с которых компьютер виден в сети.



- **Последнее соединение с Сервером.** Дата и время последнего соединения компьютера с Сервером администрирования.
- **IP-адрес.** Сетевой адрес компьютера.
- **IP-адрес соединения.** Сетевой адрес, под которым компьютер подключается к Серверу администрирования. Например, в случае подключения к Серверу администрирования через прокси-сервер это будет адрес прокси-сервера.
- Предупреждения с информацией о причинах, снижающих уровень антивирусной безопасности на компьютере (таких как устаревшие антивирусные базы или слишком большое количество невылеченных объектов на компьютере). Предупреждения отображаются, если статус компьютера имеет значение *Предупреждение* или *Критический*.



Нижняя часть окна содержит блок **Программы** с информацией о программах «Лаборатории Касперского», установленных на компьютере.

Блок **Программы** отображается только в том случае, если на компьютере установлены программы «Лаборатории Касперского»

Блок **Программы** содержит следующую информацию:

- **Название программы.** Полное название программы.
- Свойства программы, такие как версия программы или дата последнего обновления. Список свойств программы отображается под строкой с названием программы. Каждая программа имеет собственный список свойств.

Чтобы просмотреть свойства программы, вы можете использовать следующие элементы интерфейса:

- значок  – раскрытие блока информации со свойствами программы;
- значок  – сворачивание блока информации со свойствами программы.

## СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Просмотр списка компьютеров .....	<a href="#">21</a>

# УСТАНОВКА ПРОГРАММ НА КОМПЬЮТЕРЫ СЕТИ

В разделе содержатся инструкции о том, как устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры сети организации в режимах удаленной и локальной установки.

## В ЭТОМ РАЗДЕЛЕ

---

Об установке программ.....	<a href="#">26</a>
Об агенте обновлений .....	<a href="#">27</a>
Об инсталляционных пакетах.....	<a href="#">27</a>
Режим удаленной установки .....	<a href="#">28</a>
Режим локальной установки.....	<a href="#">33</a>

## ОБ УСТАНОВКЕ ПРОГРАММ

С помощью Kaspersky Security Center Web-Console вы можете устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети. Список программ, доступных для установки, формирует администратор поставщика услуг.

Существуют два способа установки программы:

- *Удаленная установка* (далее также «режим удаленной установки»). С помощью удаленной установки вы можете установить программу одновременно на несколько компьютеров вашей сети. Запуск и контроль удаленной установки выполняются с помощью веб-портала программы.
- *Локальная установка* (далее также «режим локальной установки»). Локальная установка применяется, например, в случаях, когда удаленная установка завершилась неудачно. Вы можете разрешить пользователям сети организации самостоятельно выполнять локальную установку программ на своих компьютерах.

Программы, доступные для установки, хранятся на Сервере администрирования в виде инсталляционных пакетов (см. раздел «Об инсталляционных пакетах» на стр. [27](#)).

## СМ. ТАКЖЕ

---

Режим локальной установки.....	<a href="#">33</a>
Режим удаленной установки .....	<a href="#">28</a>
Удаленная установка программы.....	<a href="#">29</a>
Установка программы вручную .....	<a href="#">36</a>

## ОБ АГЕНТЕ ОБНОВЛЕНИЙ

Прежде чем устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети в режиме удаленной установки, вам нужно назначить один из компьютеров вашей сети *агентом обновлений*. Агент обновлений – это компьютер, представляющий собой промежуточный центр распространения обновлений программ и инсталляционных пакетов в пределах группы администрирования.

Агент обновлений должен отвечать следующим требованиям:

- быть включенным постоянно или большую часть времени;
- иметь постоянный доступ в интернет и к другим компьютерам той группы администрирования, в которой он распространяет обновления;
- на него должен быть установлен Антивирус Касперского.

Только после того как вы назначили один из компьютеров вашей сети агентом обновлений и установили на него Антивирус Касперского (см. раздел «Назначение компьютера агентом обновлений» на стр. [28](#)), вы можете устанавливать программы на другие компьютеры вашей сети в режиме удаленной установки.

### СМ. ТАКЖЕ

О компьютерах и группах администрирования .....	<a href="#">21</a>
Назначение компьютера агентом обновлений .....	<a href="#">28</a>

## ОБ ИНСТАЛЛЯЦИОННЫХ ПАКЕТАХ

Инсталляционный пакет – это специально подготовленный запускаемый файл, предназначенный для установки программы на клиентские компьютеры. Инсталляционный пакет создается на основании файлов, входящих в состав дистрибутива программы, и содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

Инсталляционные пакеты формируются и распространяются администратором поставщика услуг.

Инсталляционные пакеты используются для удаленной установки программ «Лаборатории Касперского» и других производителей на клиентские компьютеры при помощи системы удаленного управления Kaspersky Security Center Web-Console (см. раздел «Режим удаленной установки» на стр. [28](#)).

Вы можете устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети в режиме локальной установки (см. раздел «Режим локальной установки» на стр. [33](#)), а также разрешить пользователям вашей сети самостоятельно устанавливать на своих компьютерах программы. Для этого с помощью Kaspersky Security Center Web-Console вы можете опубликовать инсталляционные пакеты программ.

### СМ. ТАКЖЕ

Отмена публикации инсталляционного пакета .....	<a href="#">35</a>
Просмотр списка опубликованных инсталляционных пакетов .....	<a href="#">34</a>
Публикация инсталляционных пакетов .....	<a href="#">34</a>

## РЕЖИМ УДАЛЕННОЙ УСТАНОВКИ

Режим удаленной установки позволяет вам устанавливать программы «Лаборатории Касперского» и других производителей одновременно на несколько компьютеров вашей сети.

Для того чтобы функция удаленной установки стала доступна, вам нужно предварительно назначить один из компьютеров вашей сети агентом обновлений и установить на него Антивирус Касперского (см. раздел «Назначение компьютера агентом обновлений» на стр. [28](#)). После этого вы можете запускать удаленную установку программы на компьютерах вашей сети.

Kaspersky Security Center Web-Console выполняет удаленную установку программ в фоновом режиме. Во время удаленной установки вы можете пользоваться другими функциями программы, а также просматривать информацию о статусе удаленной установки для каждого из компьютеров, на которых была запущена удаленная установка.

### В ЭТОМ РАЗДЕЛЕ

Назначение компьютера агентом обновлений.....	<a href="#">28</a>
Удаленная установка программы.....	<a href="#">29</a>
Просмотр информации о статусе удаленной установки программы.....	<a href="#">32</a>

## НАЗНАЧЕНИЕ КОМПЬЮТЕРА АГЕНТОМ ОБНОВЛЕНИЙ

После того как вы выбрали, какой из компьютеров вашей сети будет использоваться в качестве агента обновлений, вам нужно установить на него Антивирус Касперского из дистрибутива, входящего в состав Kaspersky Security Center Web-Console. Первая установка Антивируса Касперского выполняется локально. После установки на компьютер Антивируса Касперского, этот компьютер автоматически становится агентом обновлений. С помощью агента обновлений вы можете управлять установкой и обновлением программ «Лаборатории Касперского» и других производителей на удаленных компьютерах вашей сети.

► Чтобы установить на компьютер Антивирус Касперского и назначить этот компьютер агентом обновлений, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Добавить компьютер**, расположенной в панели слева, запустите мастер установки программы.

Откроется окно мастера установки программы с приветственной надписью.

4. Нажмите на кнопку **Установка локально на каждый компьютер с помощью дистрибутива**.

Откроется окно **Выбор дистрибутива для загрузки**.

Если программа не обнаружила опубликованные инсталляционные пакеты, вам будет предложено опубликовать инсталляционные пакеты (см. раздел «Публикация инсталляционных пакетов» на стр. [34](#)). После публикации инсталляционных пакетов установка программы продолжится.

5. Загрузите на ваш компьютер дистрибутив Антивируса Касперского. Для этого нажмите на кнопку **Загрузить**, расположенную в строке с названием программы.

6. Нажмите на кнопку **Готово**, чтобы завершить работу мастера установки программы.
7. Скопируйте (например, с помощью внешнего носителя или по сети) загруженный дистрибутив Антивируса Касперского на компьютер вашей сети, который вы назначили в агентом обновлений. Выполните установку Антивируса Касперского из дистрибутива, следуя инструкциям мастера установки дистрибутива.

После успешной установки Антивируса Касперского на компьютер-агент обновлений, этот компьютер будет автоматически добавлен в группу администрирования **Управляемые**. В мастере установки программы при следующем запуске станет доступна функция удаленной установки программ.

Компьютер-агент обновлений отобразится в списке компьютеров после того, как вы выполните вход в веб-портал Kaspersky Security Center Web-Console или обновите список компьютеров.

Если во время установки программы на экране отобразится сообщение об ошибке, обратитесь к администратору поставщика услуг.

## УДАЛЕННАЯ УСТАНОВКА ПРОГРАММЫ

➡ Чтобы установить программу на компьютеры вашей сети в режиме удаленной установки, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Добавить компьютер**, расположенной в панели слева, запустите мастер установки программы.

Откроется окно мастера установки программы с приветственной надписью.

4. Нажмите на кнопку **Установка на один и более компьютеров по сети с помощью инсталляционного пакета**.

Откроется окно **Выбор инсталляционного пакета**.

5. Выберите из списка инсталляционный пакет программы, которую вы хотите установить, и нажмите на кнопку **Далее**.

Откроется окно со списком компьютеров вашей сети, на которые вы можете установить программу.

Если вы не назначили один из компьютеров вашей сети агентом обновлений и не установили на него Антивирус Касперского, компьютеры вашей сети не отображаются в списке компьютеров в окне мастера установки программы. В этом случае вы не можете запустить удаленную установку программы на компьютерах вашей сети.

6. Установите флажки для тех компьютеров, на которые вы хотите установить программу. Если вы хотите установить программу на все компьютеры, перечисленные в списке компьютеров, установите флажок **Имя компьютера**. Нажмите на кнопку **Далее**.

Откроется окно **Добавление учетных записей** (см. рис. ниже).

Рисунок 8. Мастер установки программы. Добавление учетных записей

7. Сформируйте список учетных записей, обладающих правами администратора на выбранных для установки компьютерах (см. рис. ниже):

- Чтобы добавить учетные записи, для каждой учетной записи выполните следующие действия:
  - a. В поле **Учетная запись** введите имя учетной записи.
  - b. В поле **Пароль** введите пароль учетной записи.
  - c. Нажмите на кнопку **Добавить**.

Добавленная учетная запись отобразится в списке учетных записей в нижней части окна.

- Чтобы изменить параметры учетной записи в списке учетных записей, выполните следующие действия:
  - a. Выберите в списке учетных записей учетную запись, параметры которой вы хотите изменить, и нажмите на кнопку **Редактировать**.
  - b. Измените имя учетной записи в поле **Учетная запись**.
  - c. Измените пароль учетной записи в поле **Пароль**.

- d. Нажмите на кнопку **Сохранить изменения** (см. рис. ниже).

Новые имя и пароль выбранной учетной записи будут сохранены

**Мастер установки программы**

Тип установки | **Инсталляционный пакет** | Компьютеры | **Учетные записи** | Установка

### Добавление учетных записей

Добавьте учетные записи, обладающие правами администратора на выбранных для установки компьютерах. Если на компьютерах уже установлен и запущен Агент администрирования, этот шаг можно пропустить.

Учетная запись:

Пароль:




- User1
- User2**
- User3

Рисунок 9. Мастер установки программы. Изменение учетной записи

- Чтобы удалить учетную запись из списка учетных записей, выберите учетную запись, которую вы хотите удалить, и нажмите на кнопку **Удалить**.
  - Чтобы изменить порядок, в котором мастер установки программы будет применять учетные записи для доступа к компьютерам при запуске на них удаленной установки, выполните следующие действия:
    - Чтобы переместить учетную запись вверх по списку учетных записей, выберите учетную запись, которую вы хотите переместить, и нажмите на кнопку **Вверх**.
    - Чтобы переместить учетную запись вниз по списку учетных записей, выберите учетную запись, которую вы хотите переместить, и нажмите на кнопку **Вниз**.
8. Запустите процесс удаленной установки программы, нажав на кнопку **Запустить**.

На выбранных компьютерах запустится процесс удаленной установки. Откроется окно **Выполняется установка <Название программы> на следующие компьютеры**, которое содержит список задач установки программы на выбранные компьютеры вашей сети.

Вы можете просматривать список задач установки, используя следующие элементы интерфейса:

- значок  – сортировка списка задач установки по выбранному полю в алфавитном порядке по возрастанию или убыванию;
- значок  – раскрытие блока с информацией о компьютере;
- значок  – сворачивание блока с информацией о компьютере.

Блок информации о компьютере, на котором была запущена удаленная установка программы, содержит следующую информацию:

- **Имя компьютера.** Имя, под которым компьютер зарегистрирован в сети.
  - **Статус.** Статус установки программы. После запуска удаленной установки на компьютере принимает значение *Установка выполняется*.
  - **IP-адрес.** Сетевой адрес компьютера.
  - **Домен.** Имя сетевого домена, в котором зарегистрирован компьютер.
9. Чтобы завершить работу мастера установки программы, нажмите на кнопку **Заккрыть окно**. Выполнение задач установки продолжится.

Компьютеры, на которых удаленная установка завершилась успешно, автоматически добавляются в группу администрирования **Управляемые**.

Удаленная установка программы может завершиться с ошибкой (если, например, на компьютере ранее уже была установлена такая программа). Задачи установки, которые завершились с ошибкой, отображаются в списке задач со статусом *Ошибка установки*. Если удаленная установка программы на одном или нескольких компьютерах завершилась с ошибкой, вы можете установить программу локально.

Вы можете запускать только одну задачу удаленной установки. Если до окончания удаленной установки вы запустите еще одну задачу удаленной установки, выполнение текущей задачи будет прервано.

## СМ. ТАКЖЕ

Об агенте обновлений .....	<a href="#">27</a>
Об установке программ.....	<a href="#">26</a>
Установка программы вручную .....	<a href="#">36</a>
Назначение компьютера агентом обновлений.....	<a href="#">28</a>

## ПРОСМОТР ИНФОРМАЦИИ О СТАТУСЕ УДАЛЕННОЙ УСТАНОВКИ ПРОГРАММЫ

Во время удаленной установки программы вы можете просмотреть информацию о статусе удаленной установки для каждого из компьютеров, на которых была запущена удаленная установка.

- ➡ **Чтобы просмотреть информацию о статусе удаленной установки программы, выполните следующие действия:**

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).



2. Выберите закладку **Инфраструктура**.

Если запущена хотя бы одна удаленная установка программы, то в панели слева отображается ссылка **Список установок**.

3. По ссылке **Список установок** откройте окно **Список активных установок**. Окно **Список активных установок** содержит список установок программ на компьютеры вашей сети.

Компьютеры в списке установок могут иметь следующие статусы:

- *Установка выполняется* – удаленная установка программы на компьютере еще не завершена.
- *Ошибка установки* – удаленная установка программы на компьютере завершена с ошибкой. Рекомендуется установить программу вручную.

## СМ. ТАКЖЕ

Удаленная установка программы.....	<a href="#">29</a>
Установка программы вручную .....	<a href="#">36</a>

## РЕЖИМ ЛОКАЛЬНОЙ УСТАНОВКИ

Вы можете устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети в режиме локальной установки. Локальная установка программ может быть выполнена двумя способами:

- Установка вручную с помощью дистрибутива. Вы можете загрузить дистрибутив программы на компьютер и выполнить *установку вручную*, следуя инструкциям мастера установки дистрибутива. Установка вручную (далее также «режим ручной установки») требует вашего непосредственного участия в установке программы на каждом из компьютеров. Вы можете разрешить пользователям вашей сети самостоятельно устанавливать программы на своих компьютерах вручную, поместив дистрибутивы программ в сетевую папку общего доступа. Учетная запись пользователя на компьютере или в сетевом домене должна иметь разрешения на установку программ на компьютере назначения.
- Установка с помощью инсталляционного пакета. Чтобы выполнить установку программы этим способом, вам нужно опубликовать инсталляционный пакет программы. После публикации Kaspersky Security Center Web-Console предоставляет ссылку на опубликованный инсталляционный пакет. Затем, используя эту ссылку, вы можете загрузить опубликованный инсталляционный пакет на компьютер и запустить его. После запуска опубликованного инсталляционного пакета установка программы выполняется автоматически. Вы можете разрешить пользователям вашей сети самостоятельно устанавливать программы на своих компьютерах с помощью опубликованных инсталляционных пакетов, передав пользователям ссылки на опубликованные инсталляционные пакеты программ (например, по электронной почте).

## В ЭТОМ РАЗДЕЛЕ

Публикация инсталляционных пакетов .....	<a href="#">34</a>
Просмотр списка опубликованных инсталляционных пакетов .....	<a href="#">34</a>
Отмена публикации инсталляционного пакета .....	<a href="#">35</a>
Установка программы с помощью опубликованного инсталляционного пакета .....	<a href="#">35</a>
Установка программы вручную .....	<a href="#">36</a>

## ПУБЛИКАЦИЯ ИНСТАЛЛЯЦИОННЫХ ПАКЕТОВ

➤ Чтобы опубликовать инсталляционные пакеты, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Добавить пакет**, расположенной в левой части окна, откройте окно **Добавление пакетов**.  
  
Откроется окно со списком инсталляционных пакетов, которые вы можете опубликовать.
4. Установите флажки для тех инсталляционных пакетов, которые вы хотите опубликовать. Если вы хотите опубликовать все инсталляционные пакеты в списке, установите флажок напротив заголовка **Название инсталляционного пакета**.
5. Нажмите на кнопку **Опубликовать**.  
  
Статус выбранных инсталляционных пакетов изменится на *Публикуется*. Начнется публикация выбранных инсталляционных пакетов.
6. Нажмите на кнопку **Закрыть**, чтобы закрыть окно **Добавление пакетов**.

Публикация инсталляционных пакетов продолжится в автоматическом режиме. После завершения публикации инсталляционные пакеты будут добавлены в список опубликованных инсталляционных пакетов.

Опубликованные инсталляционные пакеты хранятся на Сервере администрирования. Kaspersky Security Center Web-Console предоставляет ссылки для загрузки опубликованных инсталляционных пакетов. Вы можете передать эти ссылки пользователям вашей сети.

### СМ. ТАКЖЕ

Об инсталляционных пакетах.....	<a href="#">27</a>
Отмена публикации инсталляционного пакета .....	<a href="#">35</a>
Просмотр списка опубликованных инсталляционных пакетов .....	<a href="#">34</a>

## ПРОСМОТР СПИСКА ОПУБЛИКОВАННЫХ ИНСТАЛЛЯЦИОННЫХ ПАКЕТОВ

➤ Чтобы просмотреть список опубликованных инсталляционных пакетов, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Список пакетов**, расположенной в левой части окна, откройте окно **Список инсталляционных пакетов**.

Откроется окно со списком опубликованных инсталляционных пакетов.

Список содержит следующую информацию об опубликованных инсталляционных пакетах:

- **Название инсталляционного пакета.** Название опубликованного инсталляционного пакета.
- **Постоянная ссылка на инсталляционный пакет.** Ссылка, по которой опубликованный инсталляционный пакет доступен для загрузки из локальной сети.

Если на Сервере администрирования доступна более новая версия инсталляционного пакета, вы можете обновить пакет с помощью кнопки **Обновить**, расположенной напротив инсталляционного пакета.

Вы можете передать ссылки на опубликованные инсталляционные пакеты пользователям вашей сети (например, по электронной почте). Пользователи вашей сети могут использовать их для загрузки опубликованных инсталляционных пакетов на свои компьютеры и для установки программ.

## СМ. ТАКЖЕ

Об инсталляционных пакетах.....[27](#)

## ОТМЕНА ПУБЛИКАЦИИ ИНСТАЛЛЯЦИОННОГО ПАКЕТА

Вы можете отменить публикацию инсталляционного пакета (например, если его версия устарела).

➡ Чтобы отменить публикацию инсталляционного пакета, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Список пакетов**, расположенной в левой части окна, откройте окно **Список инсталляционных пакетов**.

Откроется окно со списком опубликованных инсталляционных пакетов.

4. Найдите в списке инсталляционный пакет, публикацию которого вы хотите отменить, и нажмите на кнопку **Закрыть доступ** в его строке.

В строке появится надпись *пакет удален, доступ закрыт*. Публикация выбранного инсталляционного пакета будет отменена. Пакет перестанет быть доступен для загрузки.

5. Чтобы закрыть окно **Список инсталляционных пакетов**, нажмите на кнопку **Закрыть**.

После отмены публикации инсталляционный пакет удаляется с Сервера администрирования и перестает быть доступен для загрузки. Ссылка на инсталляционный пакет становится недействительной.

## СМ. ТАКЖЕ

Об инсталляционных пакетах.....[27](#)

## УСТАНОВКА ПРОГРАММЫ С ПОМОЩЬЮ ОПУБЛИКОВАННОГО ИНСТАЛЛЯЦИОННОГО ПАКЕТА

➡ Чтобы установить программу с помощью опубликованного инсталляционного пакета, выполните следующие действия:

1. Загрузите опубликованный инсталляционный пакет программы на компьютер, на котором вы хотите установить программу. Для этого используйте ссылку, полученную после публикации инсталляционного пакета.

Ссылку, по которой опубликованный инсталляционный пакет доступен для загрузки из локальной сети, можно найти в списке опубликованных пакетов (см. раздел «Просмотр списка опубликованных инсталляционных пакетов» на стр. [34](#)).

2. Запустите опубликованный инсталляционный пакет. После запуска установка программы выполняется автоматически.
3. Дождитесь завершения установки программы.

## УСТАНОВКА ПРОГРАММЫ ВРУЧНУЮ

► Чтобы установить программу вручную, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. По ссылке **Добавить компьютер**, расположенной в панели слева, запустите мастер установки программы.

Откроется окно мастера установки программы с приветственной надписью.

4. Нажмите на кнопку **Установка локально на каждый компьютер с помощью загружаемого дистрибутива**.

Откроется окно **Выбор дистрибутива для загрузки**.

Если программа не обнаружила опубликованные инсталляционные пакеты, вам будет предложено опубликовать инсталляционные пакеты (см. раздел «Публикация инсталляционных пакетов» на стр. [34](#)). После публикации инсталляционных пакетов установка программы продолжится.

5. Загрузите на ваш компьютер инсталляционный пакет программы, которую вы хотите установить. Для этого нажмите на кнопку **Загрузить** в строке с названием программы.
6. Нажмите на кнопку **Готово**, чтобы завершить работу мастера установки программы.
7. Запустите инсталляционный пакет программы на каждом компьютере, на котором вы хотите установить программу. Далее следуйте инструкциям инсталляционного пакета.

После успешной установки программы на компьютеры эти компьютеры автоматически добавляются в группу администрирования **Управляемые**.

Добавленные компьютеры отобразятся в списке компьютеров после того, как вы выполните вход в веб-портал Kaspersky Security Center Web-Console или обновите список компьютеров.

Если во время установки программы на экране отобразится сообщение об ошибке, обратитесь к администратору поставщика услуг.

## СМ. ТАКЖЕ

Об установке программ.....	<a href="#">26</a>
Просмотр списка компьютеров.....	<a href="#">21</a>
Процесс подключения к Серверу администрирования .....	<a href="#">14</a>
Назначение компьютера агентом обновлений.....	<a href="#">28</a>

# УПРАВЛЕНИЕ ПОЛИТИКАМИ

*Политика* – это набор параметров работы программы, определенный для группы администрирования. При помощи политик централизованно устанавливаются единые значения параметров работы программы для всех клиентских компьютеров в группе администрирования, а также запрещается изменение параметров локально через интерфейс программы. Политика определяет не все параметры программы.

Для одной программы может быть определено несколько политик с различными значениями параметров, но активная политика для программы может быть только одна. Предусмотрена возможность активировать политику, не являющуюся активной, при наступлении события, что позволяет, например, устанавливать более жесткие параметры антивирусной защиты в периоды вирусных эпидемий.

Для разных групп параметры работы программы могут быть различными. В каждой группе может быть создана собственная политика для программы.

Также могут быть сформированы политики для автономных пользователей. Если происходит разрыв соединения между Сервером администрирования и клиентским компьютером, на клиентском компьютере вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

После удаления политики или прекращения ее действия программа продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры можно изменить вручную.

## В ЭТОМ РАЗДЕЛЕ

Просмотр списка политик .....	<a href="#">37</a>
Активация политики .....	<a href="#">38</a>
Применение политики для автономных пользователей.....	<a href="#">39</a>
Удаление политики.....	<a href="#">39</a>

## ПРОСМОТР СПИСКА ПОЛИТИК

Вы можете просмотреть список политик, сформированных для компьютеров вашей сети, находящихся под управлением Сервера администрирования. Вы можете просмотреть списки политик отдельно для каждой из групп администрирования.

➡ Чтобы просмотреть список политик, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. В открывшемся окне выберите закладку **Политики**.
4. В левой части окна выберите группу администрирования, список политик которой вы хотите просмотреть.

На экране отобразится список политик выбранной группы администрирования (см. рис. ниже).

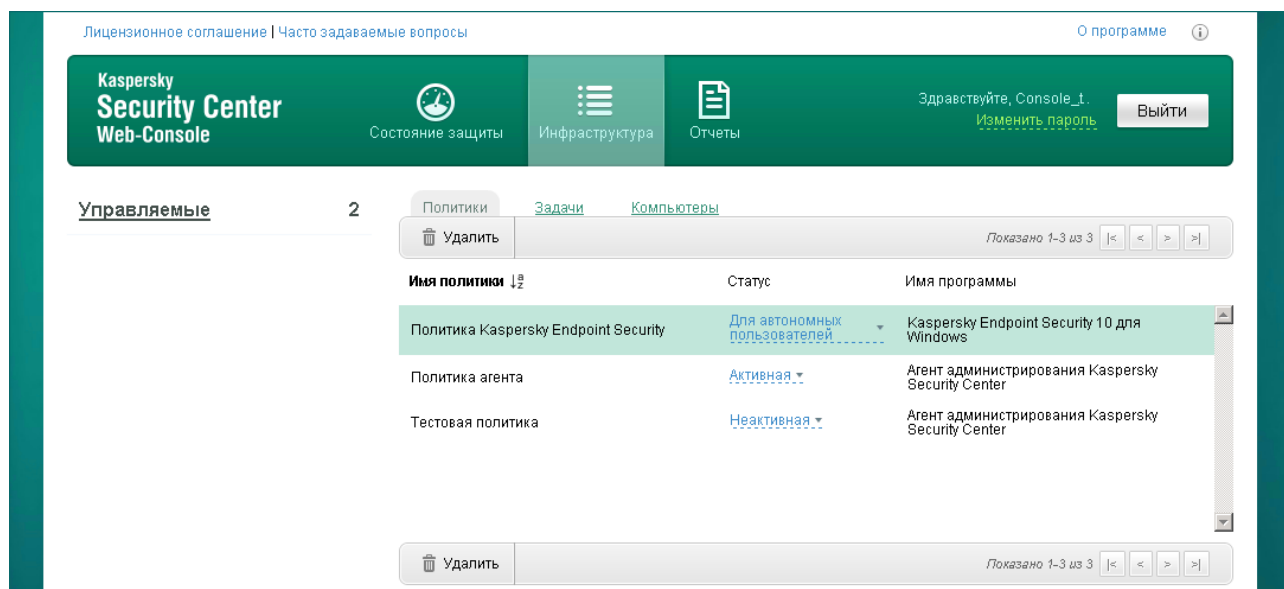




Рисунок 10. Просмотр списка политик

Список политик содержит следующую информацию о политиках:

- имя политики;
- статус политики (активная, неактивная, для автономных пользователей);
- имя программы, для которой создана политика.

Чтобы просмотреть информацию о конкретной политике, вы можете найти ее в списке политик, используя следующие элементы интерфейса:

- кнопки  – переход к следующей / предыдущей, первой / последней странице списка политик;
- значок  в заголовке графы – сортировка записей в списке политик в алфавитном порядке по возрастанию или убыванию значения графы.

## АКТИВАЦИЯ ПОЛИТИКИ

➡ Чтобы сделать политику активной для выбранной группы администрирования, выполните следующие действия:

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. 11) на закладке **Инфраструктура** выберите закладку **Политики**.
2. Выберите в списке политику, которую вы хотите активировать.
3. В раскрывающемся списке в графе **Статус** выберите значение **Активная**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских компьютеров на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

## ПРИМЕНЕНИЕ ПОЛИТИКИ ДЛЯ АВТОНОМНЫХ ПОЛЬЗОВАТЕЛЕЙ

Политика для автономных пользователей вступает в силу на компьютере в случае его отключения от сети организации.

► Чтобы применить выбранную политику для автономных пользователей,

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)) на закладке **Инфраструктура** выберите закладку **Политики**.
2. Выберите в списке политику, которую вы хотите применить для автономных пользователей.
3. В раскрывающемся списке в графе **Статус** выберите значение **Для автономных пользователей**.

В результате политика начинает действовать на компьютерах в случае их отключения от сети организации.

## УДАЛЕНИЕ ПОЛИТИКИ

► Чтобы удалить политику, выполните следующие действия:

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)) на закладке **Инфраструктура** выберите закладку **Политики**.
2. Выберите в списке политику, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтвердите выполнение операции, нажав на кнопку **Да**.

В результате политика будет удалена из списка.

# УПРАВЛЕНИЕ ЗАДАЧАМИ

Сервер администрирования управляет работой программ, установленных на клиентских компьютерах, путем создания и запуска задач. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Для каждой программы может быть создано любое количество задач.

Вы можете запускать и останавливать задачи, просматривать результаты их выполнения, а также удалять задачи.

Результаты выполнения задач сохраняются как централизованно на Сервере администрирования, так и локально на каждом клиентском компьютере.

## В ЭТОМ РАЗДЕЛЕ

---

Просмотр списка задач .....	<a href="#">40</a>
Запуск и остановка задачи вручную.....	<a href="#">42</a>
Просмотр результатов выполнения задачи .....	<a href="#">42</a>
Удаление задачи .....	<a href="#">42</a>

## ПРОСМОТР СПИСКА ЗАДАЧ

Вы можете просматривать список задач, сформированных для компьютеров вашей сети, находящихся под управлением Сервера администрирования. Вы можете просматривать списки задач отдельно для каждой из групп администрирования.

► Чтобы просмотреть список задач, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Инфраструктура**.
3. В открывшемся окне выберите закладку **Задачи**.
4. В левой части окна выберите группу администрирования, список задач которой вы хотите просмотреть.



На экране отобразится список задач выбранной группы администрирования (см. рис. ниже).

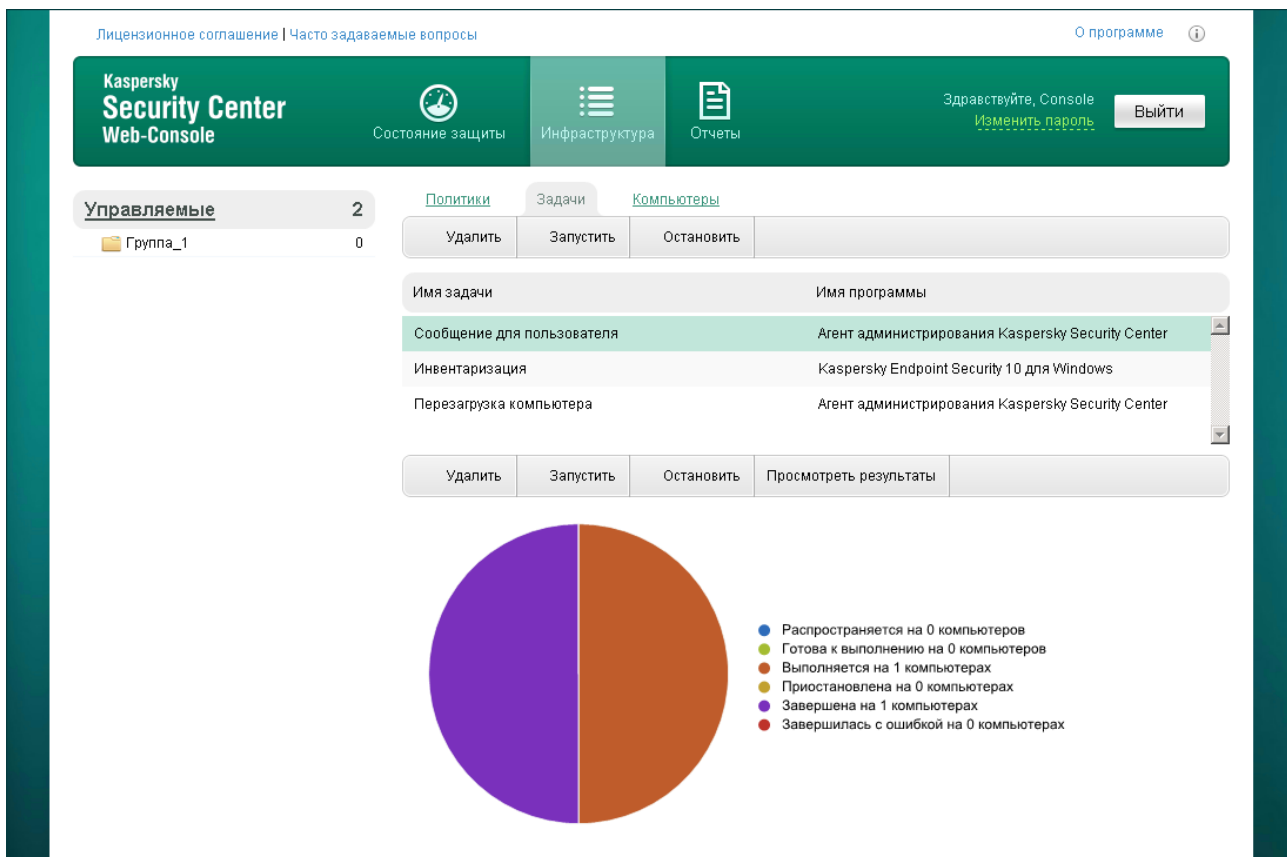




Рисунок 11. Просмотр списка задач

Список задач содержит следующую информацию о задачах:

- имя задачи;
- имя программы, для которой создана задача.

В нижней части окна отображается статистика выполнения задачи, выделенной в списке задач.

Чтобы просмотреть информацию о конкретной задаче, вы можете найти ее в списке задач, используя следующие элементы интерфейса:

- кнопки  – переход к следующей / предыдущей, первой / последней странице списка задач;
- значок  в заголовке графы – сортировка записей в списке задач в алфавитном порядке по возрастанию или убыванию значения графы.

## ЗАПУСК И ОСТАНОВКА ЗАДАЧИ ВРУЧНУЮ

➤ Чтобы запустить или остановить задачу вручную, выполните следующие действия:

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)) на закладке **Инфраструктура** выберите закладку **Задачи**.
2. Выберите в списке задачу, которую вы хотите остановить или запустить.
3. Нажмите на кнопку **Запустить** или **Остановить**.

В результате задача будет запущена или остановлена.

Запуск задач на клиентском компьютере выполняется только в том случае, если запущена программа, для которой созданы эти задачи. При остановке программы выполнение всех запущенных задач прекращается.

## ПРОСМОТР РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ ЗАДАЧИ

➤ Чтобы посмотреть результаты выполнения задачи,

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)) на закладке **Инфраструктура** выберите закладку **Задачи**.
2. В списке задач выберите задачу, результаты выполнения которой вы хотите посмотреть.
3. Нажмите на кнопку **Просмотреть результаты**.

В открывшемся окне отобразятся результаты выполнения выбранной задачи.

## УДАЛЕНИЕ ЗАДАЧИ

➤ Чтобы удалить задачу, выполните следующие действия:

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)) на закладке **Инфраструктура** выберите закладку **Задачи**.
2. В списке задач выберите задачу, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтвердите удаление задачи, нажав на кнопку **Да**.

В результате задача будет удалена из списка.

# РАБОТА С ОТЧЕТАМИ

Этот раздел содержит инструкции о том, как производить следующие операции с отчетами Сервера администрирования, к которому подключена программа: просматривать, распечатывать, отправлять по электронной почте и сохранять данные отчетов в файл.

## В ЭТОМ РАЗДЕЛЕ

Об отчетах .....	<a href="#">43</a>
Действия над отчетами .....	<a href="#">43</a>
Просмотр отчетов .....	<a href="#">44</a>
Экспорт отчета .....	<a href="#">45</a>
Настройка параметров рассылки отчетов .....	<a href="#">45</a>

## ОБ ОТЧЕТАХ

Kaspersky Security Center Web-Console позволяет получать доступ к отчетам Сервера администрирования, к которому подключена программа.

В отчетах содержится разнообразная информация о состоянии системы защиты компьютеров, находящихся под управлением Сервера администрирования.

Список доступных для вас отчетов формирует администратор поставщика услуг. В зависимости от прав доступа, назначенных вашей учетной записи, список отчетов может изменяться.

## ДЕЙСТВИЯ НАД ОТЧЕТАМИ

Вы можете производить над отчетами Сервера администрирования следующие действия:

- **Просматривать отчеты.**

Вы можете просматривать отчеты, опубликованные для вас администратором поставщика услуг. Содержимое отчетов доступно только для чтения. Вы не можете изменять отчеты.

- **Экспортировать отчеты.**

Просматривая отчет, вы можете экспортировать отчет и сохранить его, например, для последующего анализа или обработки. Вы можете экспортировать отчет в одном из трех форматов: HTML, XML или PDF.

- **Настраивать параметры автоматической рассылки отчетов по электронной почте.**

Сервер администрирования позволяет автоматически рассылать отчеты по электронной почте. Вам может потребоваться настроить рассылку отчетов так, чтобы Kaspersky Security Center Web-Console доставлял их на ваш адрес электронной почты, а также на адреса электронной почты сотрудников, которые могут быть заинтересованы в получении информации о состоянии антивирусной безопасности вашей сети (например, системные администраторы вашей сети или другие IT-специалисты).

Вы можете управлять автоматической рассылкой отчетов, настраивая параметры рассылки: набор рассылаемых отчетов и список электронных адресов получателей. Все получатели, перечисленные в списке, получают одинаковый набор отчетов.

Сервер администрирования рассылает отчеты один раз в сутки, в 00:00 часов.

СМ. ТАКЖЕ

Просмотр отчетов.....44

Экспорт отчета.....45

Настройка параметров рассылки отчетов .....45

ПРОСМОТР ОТЧЕТОВ

- ➡ Чтобы просмотреть отчет, выполните следующие действия:
- 1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 11).
  - 2. Выберите закладку **Отчеты**.
  - 3. В списке отчетов в левой части окна выберите отчет, который вы хотите просмотреть (см. рис. ниже).

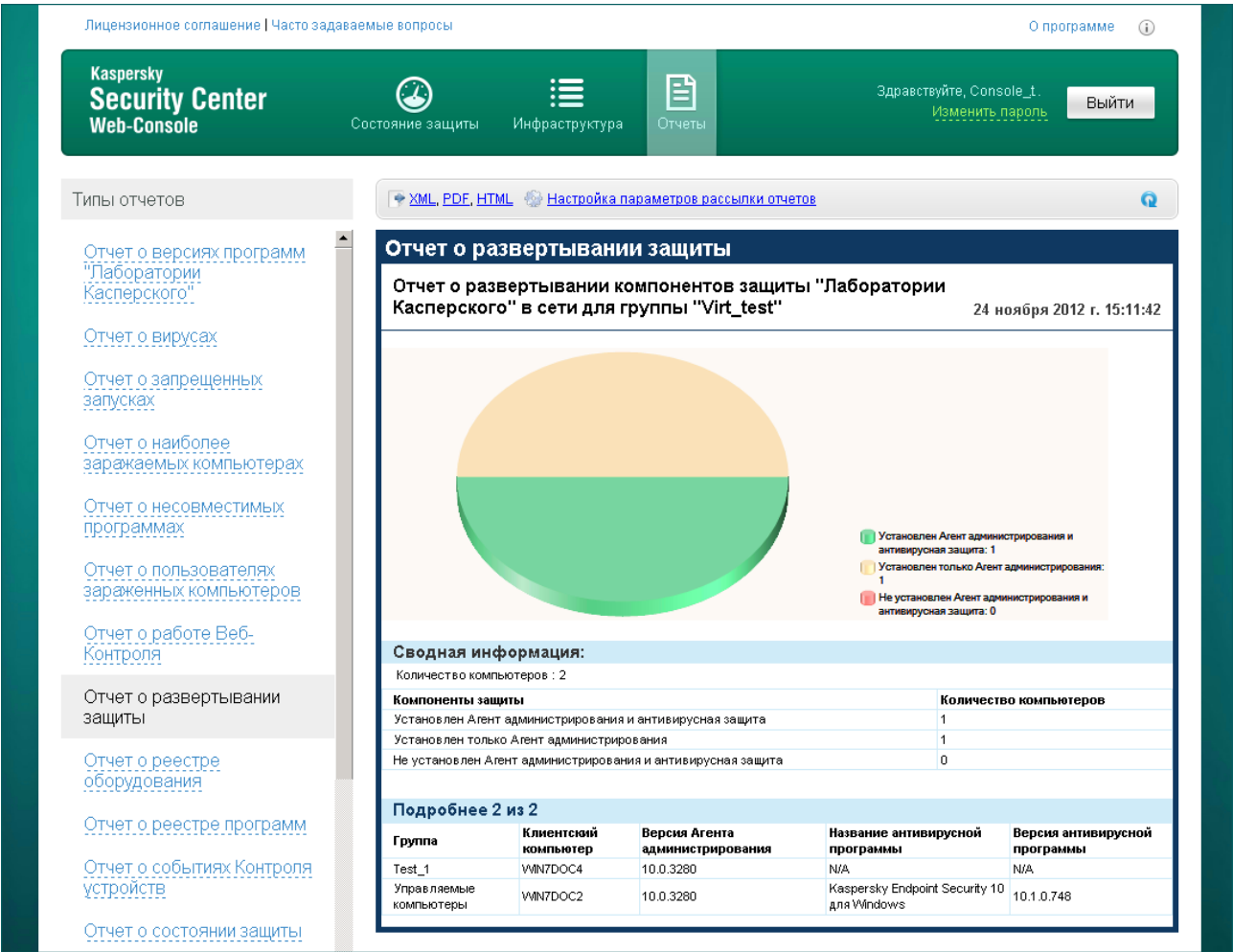



Рисунок 12. Просмотр отчетов

Содержимое отчета отобразится в правой части окна. В правом верхнем углу окна отображаются дата и время создания отчета.

Вы можете обновить содержимое отчета, чтобы просмотреть более свежие данные.

➤ Чтобы обновить содержимое отчета,

нажмите на кнопку , расположенную в правом верхнем углу окна.

## ЭКСПОРТ ОТЧЕТА

➤ Чтобы экспортировать отчет, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Отчеты**.
3. Выберите из списка отчетов в левой части окна отчет, который вы хотите экспортировать.

Содержимое отчета отобразится в правой части окна.

4. Перейдите по одной из ссылок, расположенных в верхней части окна:

- если вы хотите экспортировать отчет в формат XML, используйте ссылку **XML**;
- если вы хотите экспортировать отчет в формат PDF, используйте ссылку **PDF**;
- если вы хотите экспортировать отчет в формат HTML, используйте ссылку **HTML**.

Отчет в выбранном формате откроется в окне браузера или в окне программы просмотра, которая ассоциирована в вашей операционной системе с выбранным форматом (такой как Acrobat Reader для формата PDF).

5. Сохраните отчет в файл средствами браузера или программы просмотра.


## НАСТРОЙКА ПАРАМЕТРОВ РАССЫЛКИ ОТЧЕТОВ

➤ Чтобы настроить параметры рассылки отчетов по электронной почте, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Выберите закладку **Отчеты**.
3. Откройте окно **Настройка параметров рассылки отчетов**, перейдя по ссылке, расположенной в верхней части главного окна.
4. В списке отчетов установите флажки рядом с названиями отчетов, которые вы хотите включить в рассылку. Если вы хотите включить в рассылку все отчеты, установите флажок **Тип отчета**.
5. Сформируйте список адресов электронной почты получателей (далее – «список рассылки»):

- Чтобы добавить адрес электронной почты в список рассылки, выполните следующие действия:

- a. Введите адрес электронной почты в поле **Адрес получателя**.

- b. Нажмите на кнопку .

Новый адрес электронной почты отобразится в списке рассылки.

- Чтобы удалить адрес электронной почты из списка рассылки, выберите адрес, который вы хотите удалить, и нажмите на кнопку **Удалить**.
- Чтобы изменить адрес электронной почты в списке рассылки, выполните следующие действия:
  - а. Выберите в списке рассылки адрес электронной почты, который вы хотите изменить.

Выбранный адрес электронной почты отобразится в поле **Адрес получателя**.

- б. Измените адрес электронной почты в поле **Адрес получателя** и нажмите на кнопку .

Измененный адрес электронной почты отобразится в списке рассылки.

6. Нажмите на кнопку **Сохранить**.

Параметры рассылки отчетов немедленно вступят в действие.

# СМЕНА ПАРОЛЯ УЧЕТНОЙ ЗАПИСИ

Вы можете сменить пароль вашей учетной записи после входа в Kaspersky Security Center Web-Console. Вам может потребоваться сменить пароль, если, например, вы хотите установить для вашей учетной записи пароль, более удобный для запоминания.

► Чтобы сменить пароль учетной записи, выполните следующие действия:

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. [11](#)).
2. Перейдите по ссылке **Сменить пароль**, расположенной справа сверху, и откройте окно **Смена пароля**.
3. В полях **Новый пароль** и **Подтверждение пароля** введите новый пароль.
4. Нажмите на кнопку **Сменить пароль**.

Пароль вашей учетной записи будет изменен.

# ВЫХОД ИЗ KASPERSKY SECURITY CENTER WEB-CONSOLE

Вы можете выйти из Kaspersky Security Center Web-Console, находясь на любой закладке программы.

Для выхода из программы следует завершить сеанс работы с Kaspersky Security Center Web-Console.

Если вы выйдете из веб-браузера, не завершив сеанс работы (например, закрыв окно или вкладку веб-браузера), то сеанс будет оставаться активным в течение 24-х часов после выхода.

➡ Чтобы завершить сеанс работы с Kaspersky Security Center Web-Console,

находясь в главном окне программы (см. раздел «Интерфейс программы» на стр. [11](#)), нажмите на кнопку **Выйти**, расположенную в правом верхнем углу окна.

Сеанс работы с Kaspersky Security Center Web-Console будет завершен. В веб-браузере откроется окно ввода имени пользователя и пароля (см. раздел «Процесс подключения к Серверу администрирования» на стр. [14](#)).



# ГЛОССАРИЙ

## Н

### HTTPS

Безопасный протокол передачи данных между браузером и веб-сервером с использованием шифрования. HTTPS используется для доступа к закрытой информации, такой как корпоративные или финансовые данные.

## Ж

### JAVASCRIPT

Язык программирования, расширяющий возможности веб-страниц. Веб-страницы, созданные с использованием JavaScript, способны выполнять дополнительные действия (например, изменять вид элементов интерфейса или открывать дополнительные окна) без обновления веб-страницы данными с веб-сервера. Чтобы просматривать веб-страницы, созданные с использованием JavaScript, в параметрах веб-браузера надо включить поддержку JavaScript.

## С

### SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

## А

### АГЕНТ ОБНОВЛЕНИЙ

Компьютер, представляющий собой промежуточный центр распространения обновлений и инсталляционных пакетов в пределах группы администрирования.

### АДМИНИСТРАТОР КЛИЕНТА

Сотрудник предприятия-клиента, который отвечает за обеспечение антивирусной безопасности организации-клиента.

### АДМИНИСТРАТОР ПОСТАВЩИКА УСЛУГ

Сотрудник организации-поставщика услуг антивирусной защиты. Выполняет работы по инсталляции, эксплуатации систем антивирусной защиты, созданных на основе решений «Лаборатории Касперского», а также осуществляет техническую поддержку клиентов.

### АНТИВИРУСНАЯ БЕЗОПАСНОСТЬ СЕТИ

Комплекс технических и организационных мер, снижающих вероятность проникновения на компьютеры сети предприятия вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании антивирусных программ и сервисов, а также при наличии и соблюдении политики информационной безопасности на предприятии.

## В

### ВЕБ-ПОРТАЛ

Средство для доступа к функциям Kaspersky Security Center Web-Console посредством веб-браузера. Веб-портал состоит из веб-страниц с текстовой и графической информацией и элементами управления функциями Kaspersky Security Center Web-Console. Веб-страницы открываются в веб-браузере после входа в веб-портал. Для входа в веб-портал необходимо иметь адрес веб-портала, имя учетной записи пользователя и пароль.

## Г

### Группа администрирования

Набор компьютеров, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ «Лаборатории Касперского». Компьютеры группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

## И

### Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы «Лаборатории Касперского» при помощи системы удаленного управления Kaspersky Security Center Web-Console. Инсталляционный пакет создается на основании специальных файлов с расширениями .kpd и .kud, входящих в состав дистрибутива программы, и содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию.

## Л

### Локальная установка

Установка антивирусной программы на компьютер сети организации, которая предусматривает ручной запуск установки из дистрибутива антивирусной программы или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на компьютер.

## П

### Поставщик услуг антивирусной защиты

Организация, предоставляющая предприятию услуги антивирусной защиты сетей организации-клиента на основе решений «Лаборатории Касперского».

## Р

### Ручная установка

Установка антивирусной программы на компьютер сети организации из дистрибутива антивирусной программы. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

## С

### Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах «Лаборатории Касперского» и управления ими.

### Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности компьютеров сети организации. Состояние защиты сети включает такие факторы, как наличие на компьютерах сети установленных антивирусных программ, использование ключей, количество и виды обнаруженных угроз.

## У

### Удаленная установка

Установка программ «Лаборатории Касперского» при помощи сервисов, предоставляемых программой Kaspersky Security Center Web-Console.

### Управляемые компьютеры

Компьютеры сети организации, включенные в одну из групп администрирования.

# ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

**Продукты.** Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежедневно, база Анти-Спама – каждые 5 минут.*

**Технологии.** Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

**Достижения.** За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:

<http://www.kaspersky.ru>

Вирусная энциклопедия:

<http://www.securelist.com/ru/>

Антивирусная лаборатория:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (только для отправки возможно зараженных файлов в архивированном виде)

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

(для запросов вирусным аналитикам)

Веб-форум «Лаборатории Касперского»:

<http://forum.kaspersky.com>

# ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Для создания программы использовался код сторонних производителей.

## В ЭТОМ РАЗДЕЛЕ

---

C++ JSON PARSER 4.03 .....	<a href="#">52</a>
FCGI-2.4.1-SNAP-0910052249 .....	<a href="#">52</a>
ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE) .....	<a href="#">53</a>
MOD_FCGI-SNAP-0910052141 .....	<a href="#">53</a>

## C++ JSON PARSER 4.03

C++ JSON Parser 4.03

Copyright (C) 2007 – 2009, John W. Wilkinson

---

The MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## FCGI-2.4.1-SNAP-0910052249

fcgi-2.4.1-SNAP-0910052249

Copyright (C) 1996, Open Market, Inc.

---

This FastCGI application library source and object code (the «Software») and its documentation (the «Documentation») are copyrighted by Open Market, Inc («Open Market»). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this

Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED «AS IS». OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

## ICU 4.4 (INTERNATIONAL COMPONENTS FOR UNICODE)

ICU 4.4 (International Components for Unicode)

Copyright (C) 1995-2010, International Business Machines Corporation and others

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## MOD\_FCGI-SNAP-0910052141

mod\_fcgi-SNAP-0910052141

Copyright (C) 1995-1996, Open Market, Inc.

This FastCGI application library source and object code (the «Software») and its documentation (the «Documentation») are copyrighted by Open Market, Inc («Open Market»). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation solely for the purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions.

No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here, but the modified Software and Documentation must be used for the sole purpose of implementing the FastCGI specification defined by Open Market or derivative specifications publicly endorsed by Open Market and promulgated by an open standards organization and for no other purpose. If modifications to this Software and Documentation have new licensing terms, the new terms must protect Open Market's proprietary rights in the Software and Documentation to the same extent as these licensing terms and must be clearly indicated on the first page of each file where they apply.

Open Market shall retain all right, title and interest in and to the Software and Documentation, including without limitation all patent, copyright, trade secret and other proprietary rights.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED «AS IS». OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

# УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Fedora и лого Infinity design – товарные знаки Red Hat, Inc.

Microsoft, Windows и Internet Explorer – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в Соединенных Штатах Америки и в других странах.

Red Hat и Red Hat Enterprise Linux – зарегистрированные в США и других странах товарные знаки Red Hat, Inc.

Mac OS, Safari, Leopard, Snow Leopard, Tiger – зарегистрированные товарные знаки Apple Inc.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

## А

Автоматическая рассылка отчетов .....	43, 46
Агенты обновлений .....	49
Администратор поставщика услуг .....	26
Антивирусная программа .....	26

## Г

Группы администрирования .....	49
--------------------------------	----

## З

ЗАО .....	51
-----------	----

## И

Инсталляционный пакет .....	26
-----------------------------	----

## К

Компьютеры	
IP-адрес .....	23
имя .....	23
нераспределенные .....	21, 23
свойства .....	23
список .....	21
управляемые .....	21, 23

## Л

ЛАБОРАТОРИЯ КАСПЕРСКОГО .....	51
-------------------------------	----

## О

Отчеты .....	43
автоматическая рассылка .....	43, 46
просмотр .....	43, 44
сохранение в файл .....	43, 45

## П

Программа антивирусная .....	26
------------------------------	----

## С

Свойства компьютера .....	23
СЕАНС РАБОТЫ .....	48
ЗАВЕРШЕНИЕ .....	48
Сервер администрирования .....	50

## У

Установка	
мастер .....	29
ручная .....	36
удаленная .....	29
УЧЕТНАЯ ЗАПИСЬ	
ПАРОЛЬ .....	47