KASPERSKY lab

Kaspersky Security Center Web Console

Руководство пользователя

Уважаемый пользователь!

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

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.

Дата редакции документа: 18.01.2016

http://www.kaspersky.ru
https://help.kaspersky.com
http://support.kaspersky.ru

Содержание

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

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

Kaspersky Security Center Web Console (см. стр. 11)

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

Программные требования (см. стр. 14)

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. 15)

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. 17)

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. 20)

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. 28)

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

Установка программ на компьютеры сети (см. стр. 35)

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. 52)

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

Управление учетными записями пользователей (см. стр. 68)

Этот раздел содержит информацию об управлении учетными записями, сформированными для пользователей вашей сети.

Управление мобильными устройствами (см. стр. 74)

Этот раздел содержит информацию об управлении мобильными устройствами, подключенными к Серверу администрирования.

Управление задачами (см. стр. 84)

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

Работа с отчетами (см. стр. 88)

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. 93)

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

Выход из Kaspersky Security Center Web Console (см. стр. 94)

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

Глоссарий терминов

Этот раздел содержит термины, используемые в документе.

АО «Лаборатория Касперского» (см. стр. 100)

Этот раздел содержит информацию о АО «Лаборатория Касперского».

Информация о стороннем коде (см. стр. 102)

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

Уведомления о товарных знаках (см. стр. 103)

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 этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример:	Примеры приведены в блоках на голубом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.

Пример текста	Описание условного обозначения
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

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 (см. стр. 20);
- устанавливать программы «Лаборатории Касперского» на компьютеры вашей сети и управлять установленными программами (см. стр. 35);
- управлять политиками, сформированными для компьютеров и мобильных устройств вашей сети (см. стр. 52);
- управлять учетными записями пользователей (см. стр. 68);
- управлять мобильными устройствами, подключенными к серверу вашей организации (см. стр. 74);
- управлять задачами для программ, установленных на компьютерах вашей сети (см. стр. 84);
- просматривать отчеты о состоянии системы безопасности (см. стр. 88);
- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам (см. стр. 88).

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 браузера (см. раздел «Программные требования» на стр. 14).

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

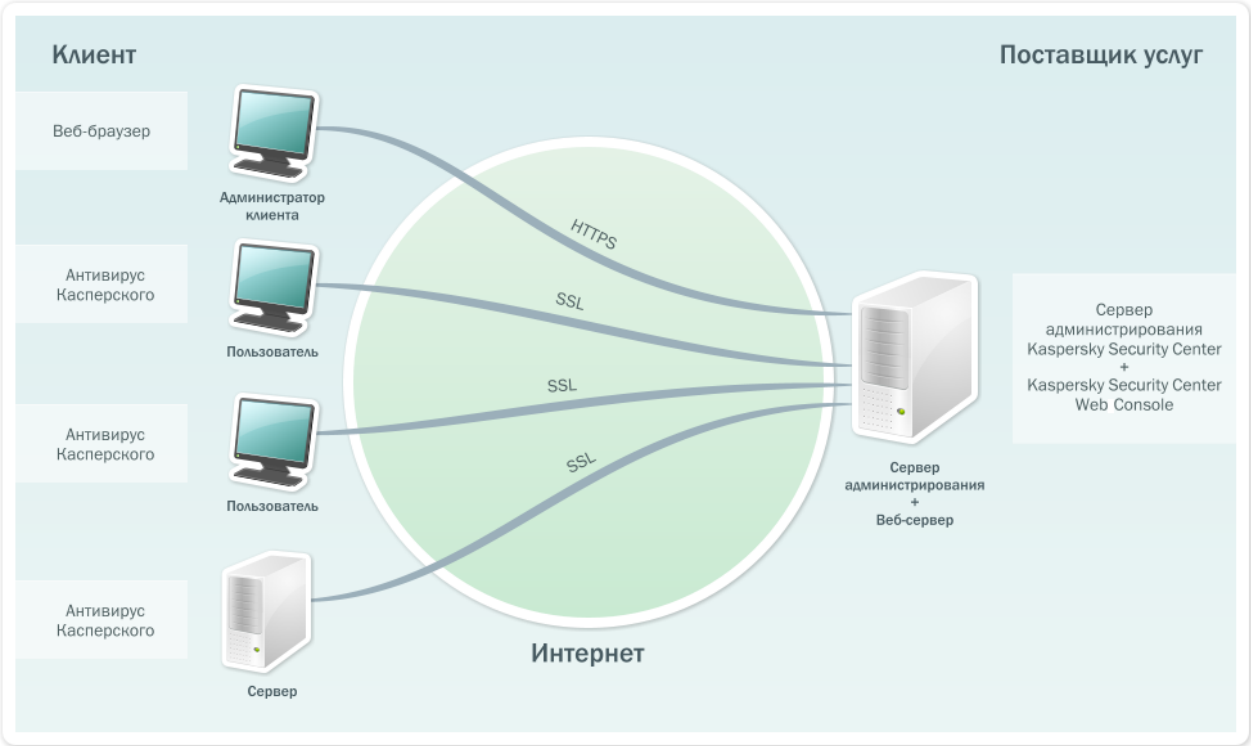

Рисунок 1. Схема работы

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 браузера. Когда вы с помощью вашего браузера подключаетесь к Kaspersky Security Center Web Console, 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 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 браузеру в удобном для отображения виде.

   - Если вы выбрали команду управления (например, удаленная установка программы), Kaspersky Security Center Web Console получает команду от браузера и передает ее Серверу администрирования. Затем программа получает результат выполнения команды от Сервера администрирования и передает результат браузеру в удобном для отображения виде.

Программные требования

Для работы с Kaspersky Security Center Web Console требуется только браузер.

Требования к аппаратному и программному обеспечению компьютера соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console поддерживает следующие браузеры:

- Internet Explorer® 9 и выше;
- Microsoft® Edge;
- Chrome™ 45 и выше;
- Firefox™ 38 и выше;
- Safari 8 и под управлением Mac OS X 10.10 (Yosemite);
- Safari 9 и под управлением Mac OS X 10.11 (El Capitan).

Вы можете получить сведения о последней версии аппаратных и программных требований на веб-сайте Службы технической поддержки, на странице Kaspersky Security Center Web Console 10, в разделе Системные требования (http://support.kaspersky.ru/ksc10#requirements).

Интерфейс программы

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

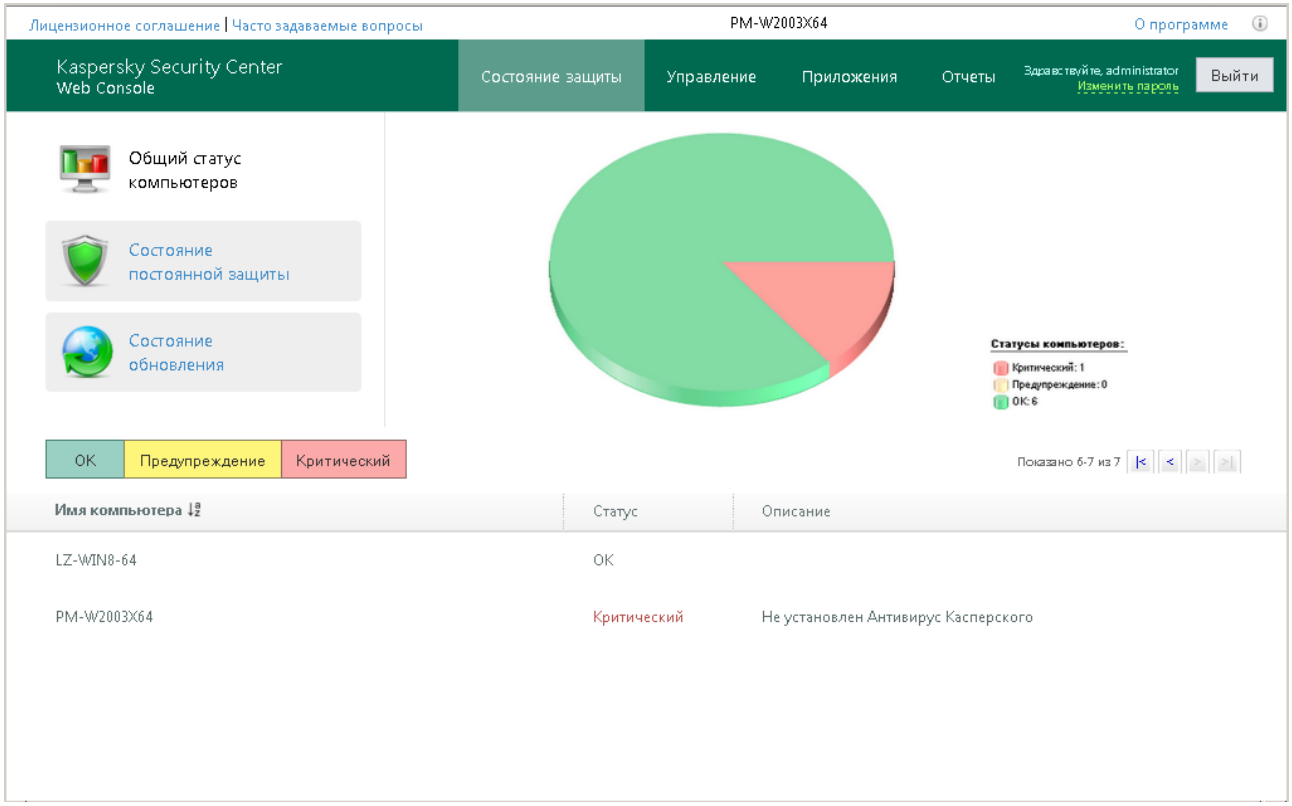

Рисунок 2. Главное окно программы

В верхней части главного окна находятся следующие элементы интерфейса:

- закладки **Состояние защиты**, **Управление**, **Приложения** и **Отчеты** – для доступа к основным функциям программы;
- значок ⓘ – для вызова контекстной справки;
- ссылка **Изменить пароль** – для смены пароля учетной записи;
- кнопка **Выйти** – 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 компьютеров**, **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.
- **Управление**. 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**.
- **Приложения**. Предназначена для публикации инсталляционных пакетов.
- **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 17

Состояние защиты сети 20

Управление компьютерами..... 28

Работа с отчетами..... 88

Выход из Kaspersky Security Center Web Console 94

Смена пароля учетной записи..... 93

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

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

Подготовка браузера

Перед подключением к Серверу администрирования вам необходимо убедиться, что в вашем 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 браузере, можно получить в документации к 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 браузер.
2. Введите в адресной строке браузера адрес веб-портала, полученный у администратора поставщика услуг (см. раздел «Подготовка к подключению к Серверу администрирования» на стр. 17). Откройте этот адрес.

   Если вы подключаетесь к Серверу администрирования в первый раз, в браузере откроется окно **Лицензионное соглашение**. Если вы ранее подключались к Серверу администрирования, в 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 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. 15).

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:

  - *OK* – 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

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

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Состояние защиты**.

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

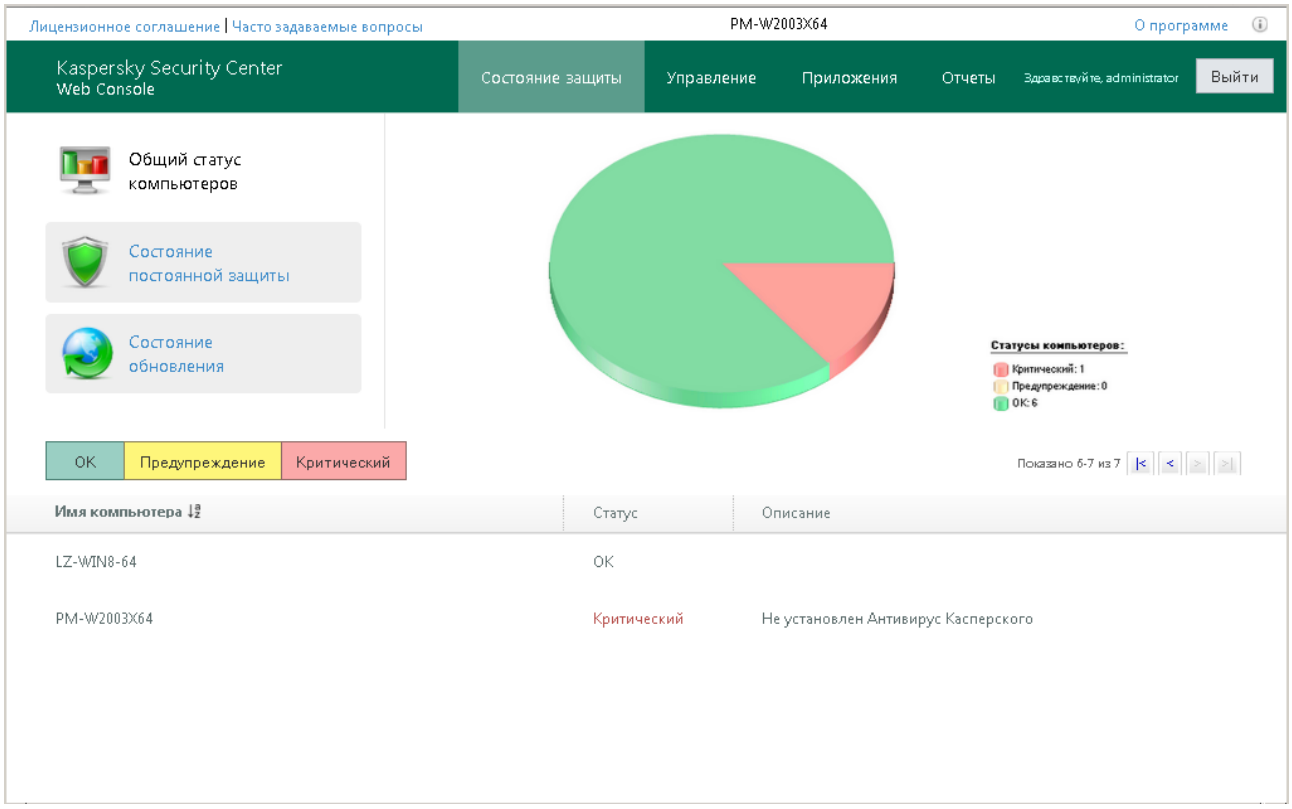

Рисунок 3. Общий статус компьютеров

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

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 по возрастанию или убыванию.

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

См. также

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. 15).
2. Выберите закладку **Состояние защиты**.
3. В левой части окна выберите раздел **Состояние постоянной защиты** (см. рис. ниже).

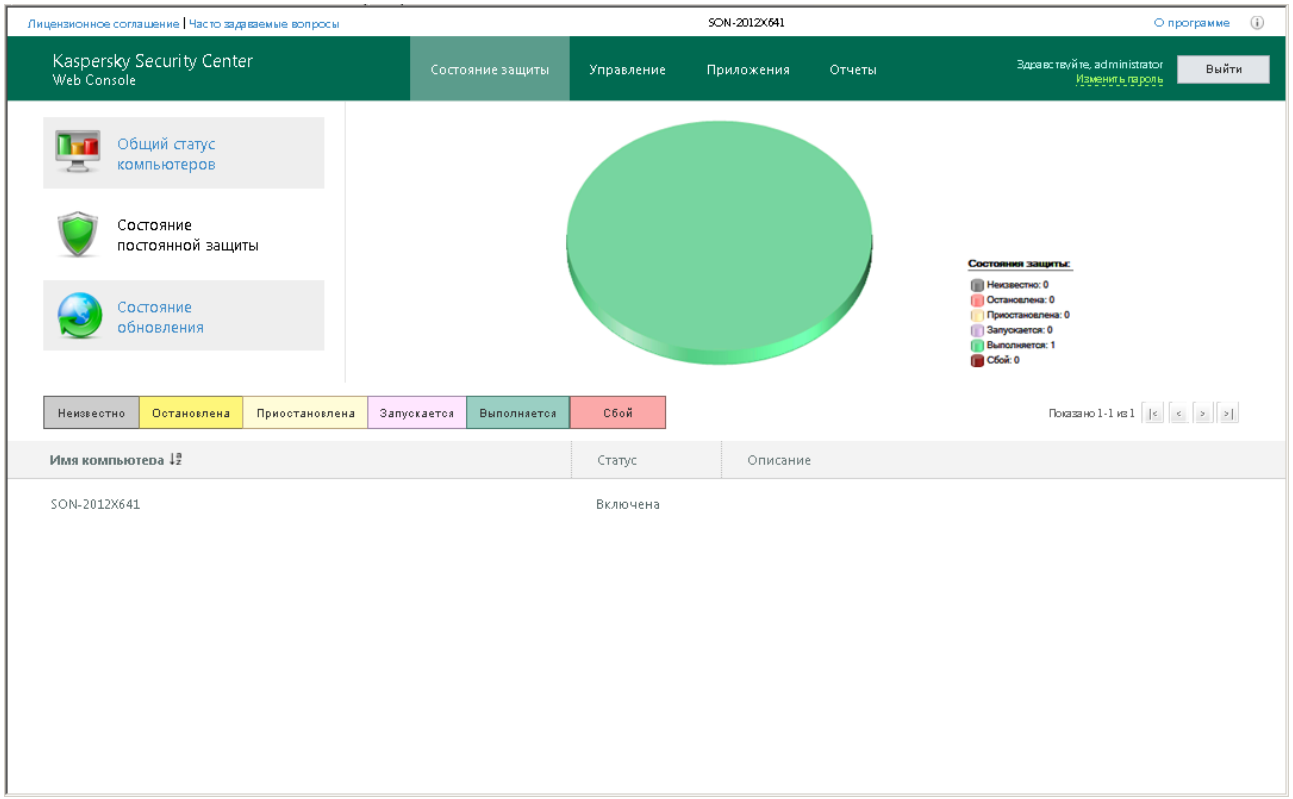

Рисунок 4. Состояние постоянной защиты

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.

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

См. также

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. 15).
2. Выберите закладку **Состояние защиты**.
3. В левой части окна выберите раздел **Состояние обновления** (см. рис. ниже).

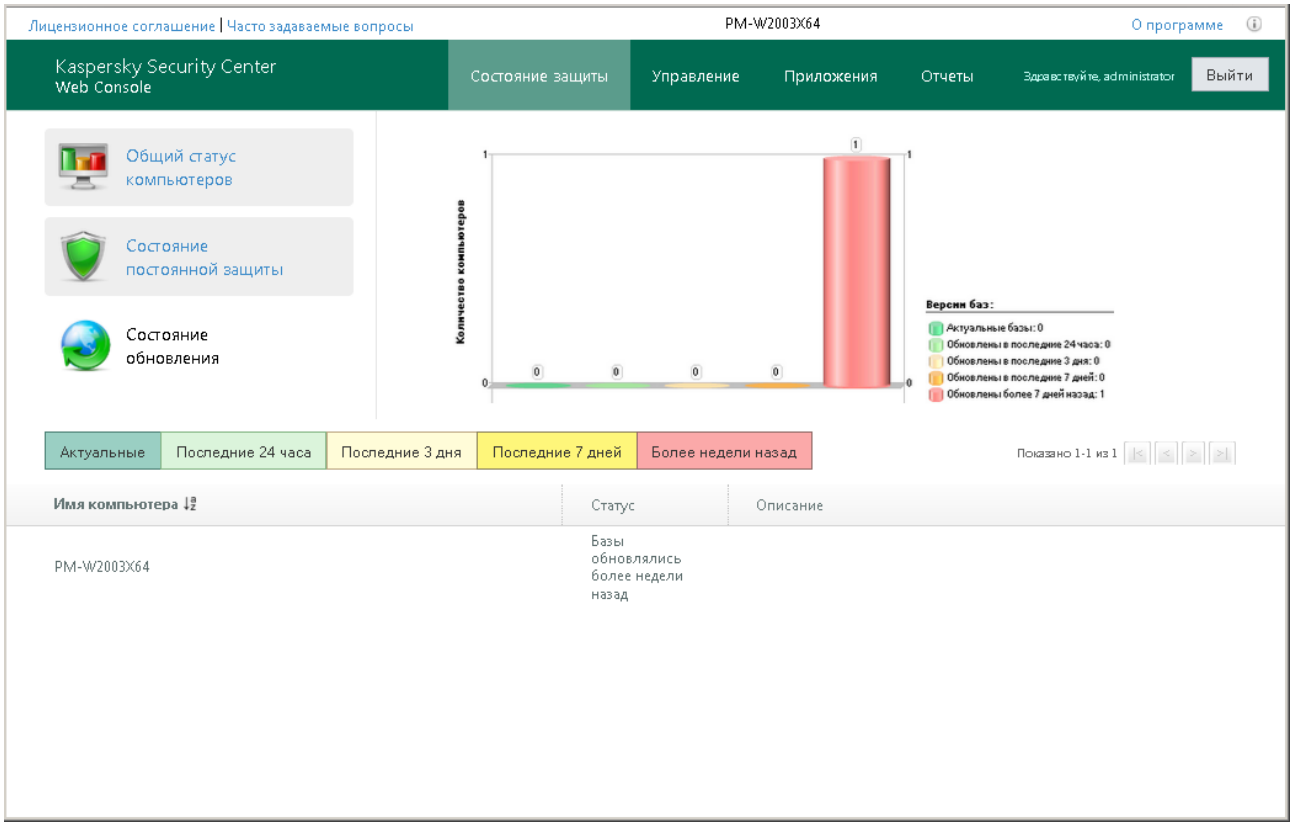

Рисунок 5. Состояние обновления

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.

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

См. также

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

Управляемые компьютеры и группы администрирования

Состояние безопасности компьютеров вашей сети контролирует Сервер 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».

Компьютеры, которые включены в какую-либо группу администрирования, называются *управляемыми компьютерами*. После установки на компьютерах вашей сети программ «Лаборатории Касперского» Сервер администрирования автоматически добавляет эти компьютеры в группу администрирования **Управляемые компьютеры**. Администратор поставщика услуг может создавать другие группы администрирования и распределять по ним компьютеры. Группы администрирования могут быть созданы внутри других групп администрирования.

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 35

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. 15).
2. Выберите закладку **Управление**.
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 компьютеры**.
   - 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 компьютеры**.

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

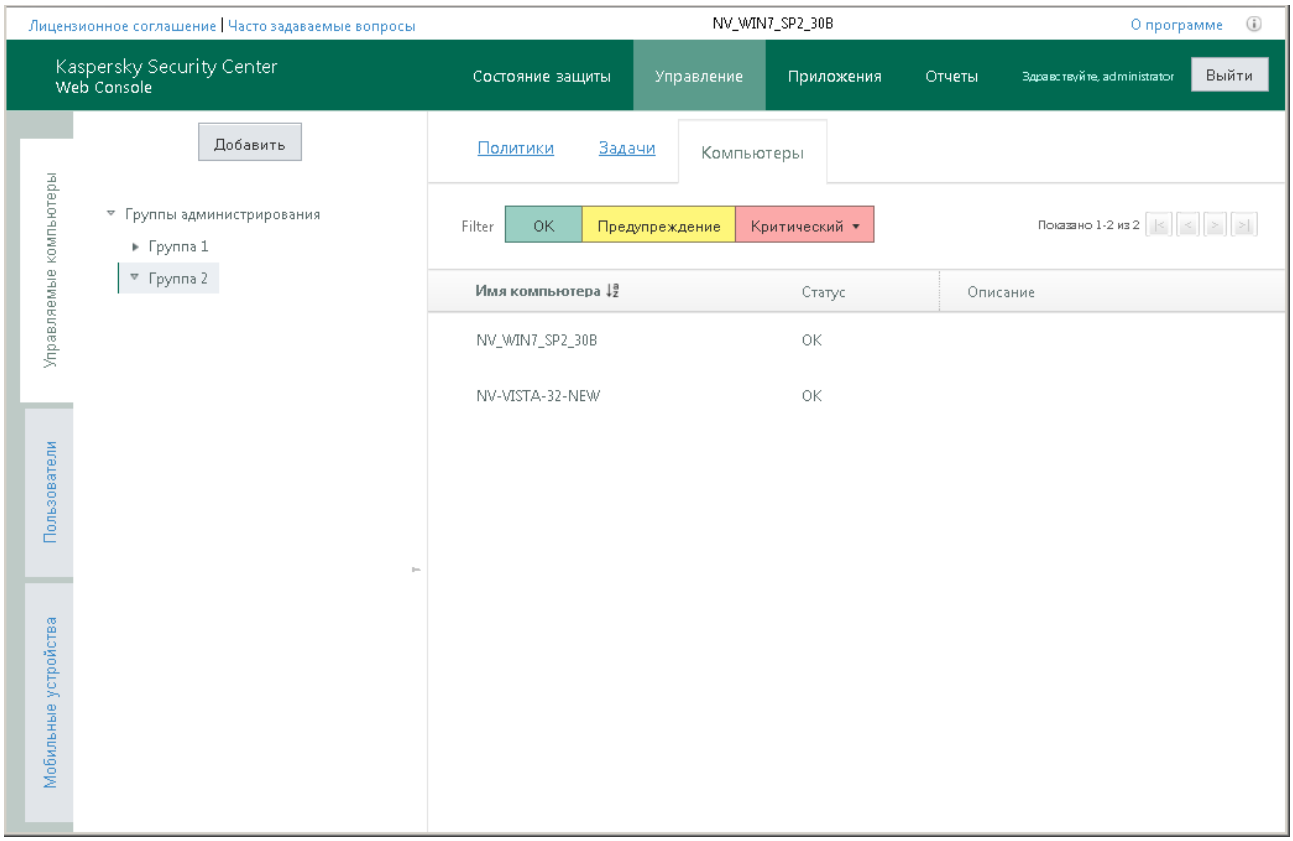

Рисунок 6. Просмотр списка компьютеров

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 по возрастанию или убыванию.

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

См. также

Управляемые компьютеры и группы администрирования 28

Состояние защиты сети 20

Просмотр свойств компьютера

► *Чтобы просмотреть свойства компьютера, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Компьютеры**.
3. Выберите в списке групп администрирования в левой части окна группу администрирования, где находится нужный 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).

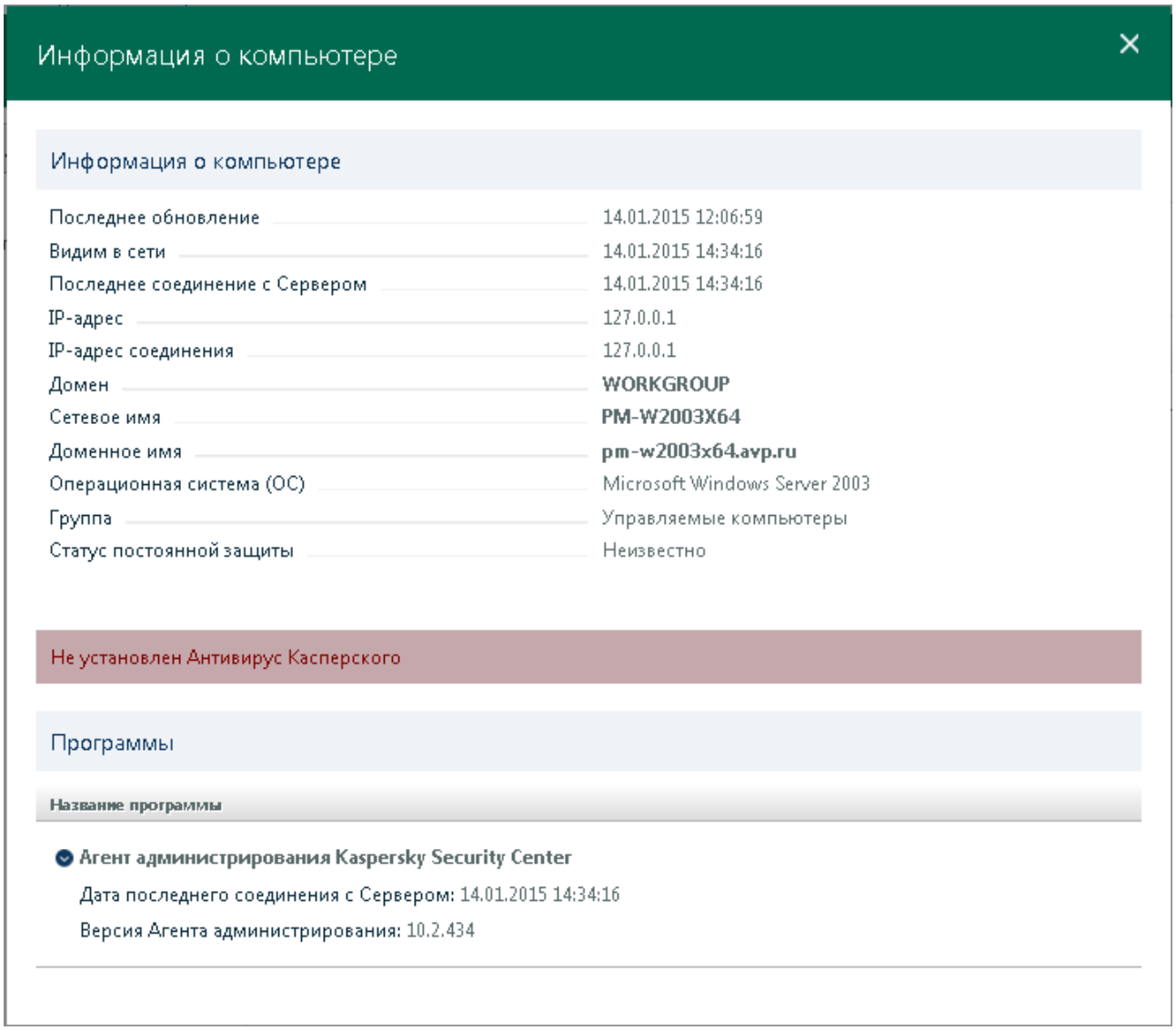

Рисунок 7. Просмотр свойств компьютера

Окно со свойствами компьютера разделено на две части.

Верхняя часть окна содержит информацию о следующих свойствах компьютера:

- **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 отображается адрес прокси-сервера.
- **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.
- 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

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

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. 36).

См. также

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.

Вы можете устанавливать программы «Лаборатории Касперского» и других производителей на компьютеры вашей сети в режиме локальной установки (см. раздел «Режим локальной установки» на стр. 41), а также разрешить пользователям вашей сети устанавливать на своих компьютерах программы самостоятельно. Для этого с помощью Kaspersky Security Center Web Console вы можете опубликовать инсталляционные пакеты программ.

См. также

Удаленная установка программ

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

► *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. 15).

2. Выберите закладку **Управление**.

3. По ссылке **Добавить**, 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.

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).

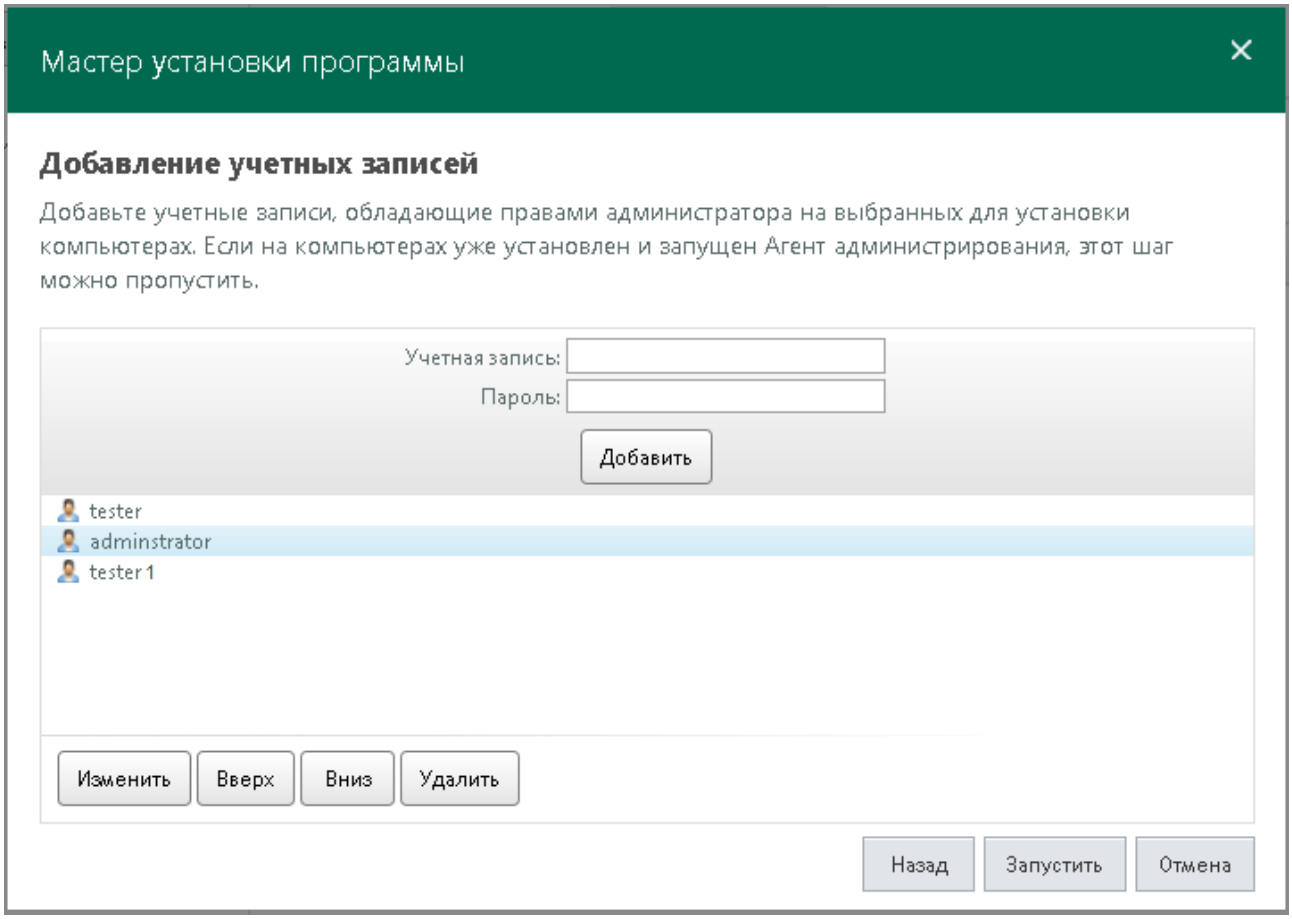

Рисунок 8. Мастер установки программы. Добавление учетных записей

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).

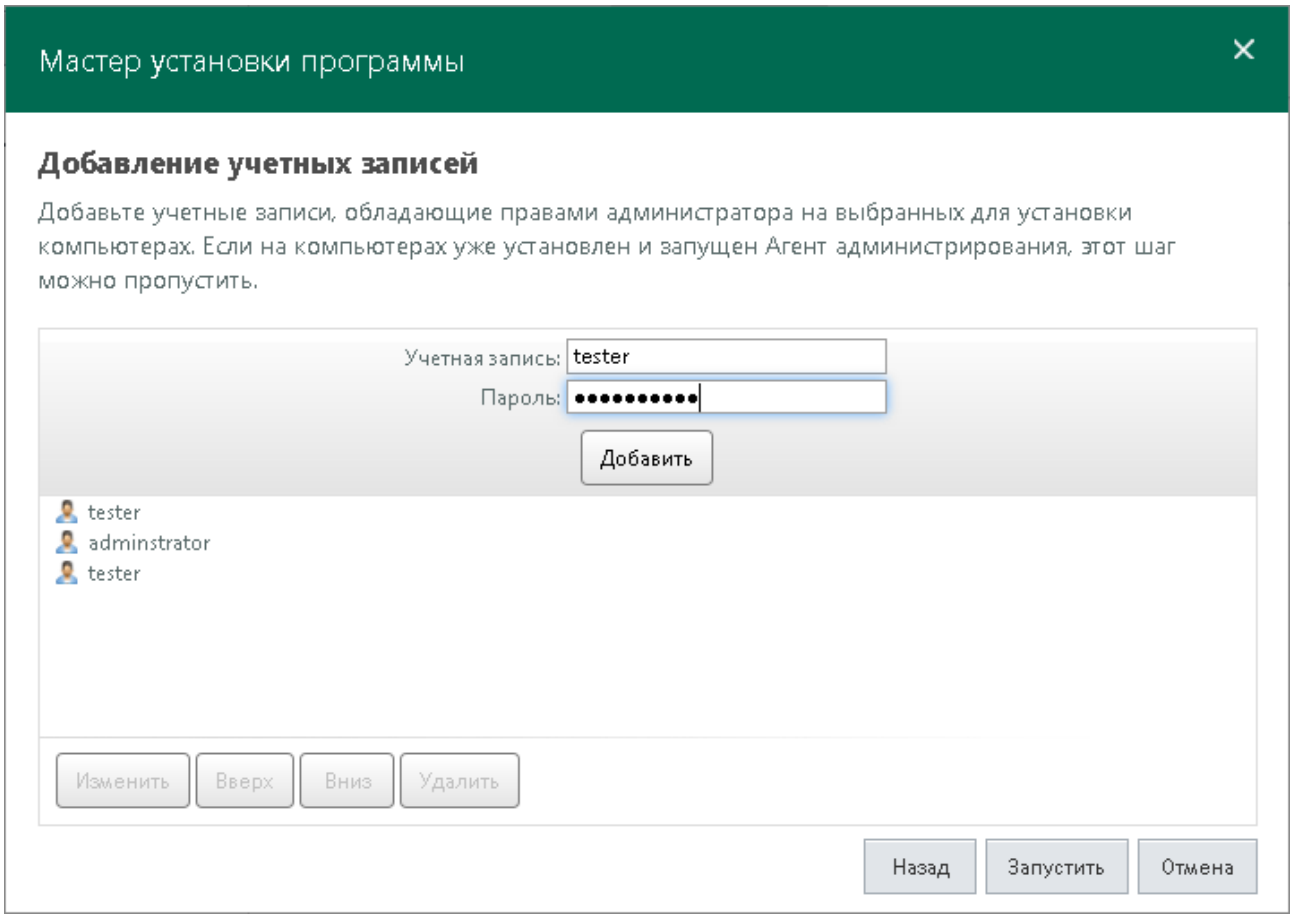

Рисунок 9. Мастер установки программы. Изменение учетной записи

Новые имя и пароль выбранной учетной записи будут сохранены.

- 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 **Закрыть окно**. Выполнение задач установки продолжится.

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

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 установке программ..... 35

Режим локальной установки

Программы «Лаборатории Касперского» и других производителей можно устанавливать на компьютеры и Android™-устройства вашей сети в режиме локальной установки. В Kaspersky Security Center Web Console предусмотрены два варианта локальной установки программ:

- Локальная установка с помощью инсталляционных пакетов. Чтобы сделать программу доступной для локальной установки, вам нужно опубликовать инсталляционный пакет программы. Опубликованные инсталляционные пакеты отображаются в главном окне программы на закладке **Приложения**. После публикации Kaspersky Security Center Web Console создает ссылку на опубликованный инсталляционный пакет. По ссылке можно загрузить опубликованный инсталляционный пакет на компьютер и запустить его. После запуска инсталляционного пакета на компьютере установка программы выполняется автоматически. Вы можете разрешить пользователям вашей сети самостоятельно устанавливать программы на своих компьютерах с помощью опубликованных инсталляционных пакетов. Для этого нужно предоставить пользователям ссылки на опубликованные инсталляционные пакеты (например, по электронной почте).
- Локальная установка из магазина приложений. Магазин приложений – это компонент Kaspersky Security Center Web Console, реализованный в интерфейсе виде отдельной закладки. Магазин приложений предназначен для размещения в нем Android-приложений и ссылок на приложения в Google Play™ с целью последующей установки на Android-устройства. Чтобы приложения стали доступны для локальной

установки, нужно добавить в корпоративный магазин приложений apk-файлы или ссылки на приложения в Google Play. Приложения в корпоративном магазине отображаются в главном окне программы на закладке **Приложения**.

В этом разделе

Публикация инсталляционных пакетов

► *Чтобы опубликовать инсталляционные пакеты, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Опубликованные пакеты** в левой части окна.
4. По кнопке **Добавить**, расположенной в верхней левой части окна, откройте окно **Мастер добавления пакетов**.

   Откроется окно со списком инсталляционных пакетов, доступных для публикации.
5. Установите флажки для тех инсталляционных пакетов, которые вы хотите опубликовать. Чтобы опубликовать все инсталляционные пакеты в списке, установите флажок напротив заголовка **Название инсталляционного пакета**.

6. Нажмите на кнопку **Опубликовать**.

   Статус выбранных инсталляционных пакетов изменится на *Публикуется*. Начнется публикация выбранных инсталляционных пакетов.

7. 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 пакетов на закладке **Опубликованные пакеты**.

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..... 36

Отмена публикации инсталляционного пакета..... 44

Просмотр списка опубликованных инсталляционных пакетов 43

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. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Опубликованные пакеты** в левой части окна.

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..... 36

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. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Опубликованные пакеты** в левой части окна.

   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.

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

См. также

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. 43).

2. Запустите опубликованный инсталляционный пакет. После запуска установка программы выполняется автоматически.

3. Дождитесь завершения установки программы.

См. также

Добавление файлов Android-приложений и ссылок на приложения в Google Play в корпоративный магазин приложений

Вы можете добавлять в магазин приложений apk-файлы приложений и ссылки на приложения в Google Play.

► *Чтобы добавить в магазин приложений apk-файл, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.
4. Нажмите на кнопку **Добавить новый пакет** над списком.

   Откроется окно **Пакет с приложением**.
5. Нажмите на кнопку **Обзор** и выберите в списке apk-файл.
6. Нажмите на кнопку **Вперед**.
7. Введите название и описание приложения в соответствующие поля ввода.

   Вы можете ввести до 256 символов в поле **Название приложения** и до 2048 символов в поле **Описание приложения**.
8. Нажмите на кнопку **Применить**.

Добавленный apk-файл отобразится в списке **Список приложений для Android**. Количество добавленных приложений отображается после заголовка списка в скобках (см. рис. ниже).

► *Чтобы добавить в магазин приложений ссылку на приложение в Google Play, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.

4. Нажмите на кнопку **Добавить ссылку на приложение в Google Play** над списком.

   Откроется окно **Ссылка на приложение в Google Play**.

5. Введите ссылку в поле ввода **Укажите ссылку на приложение**.

   Сылка должна начинаться с имени сетевого протокола **Error! Hyperlink reference not valid.**.

6. Нажмите на кнопку **Вперед**.

7. Введите название и описание приложения в соответствующие поля ввода.

   Вы можете ввести до 256 символов в поле **Название приложения** и до 2048 символов в поле **Описание приложения**.

8. Нажмите на кнопку **Применить**.

   Добавленная ссылка отобразится в списке **Список приложений для Android** (см. рис. ниже).

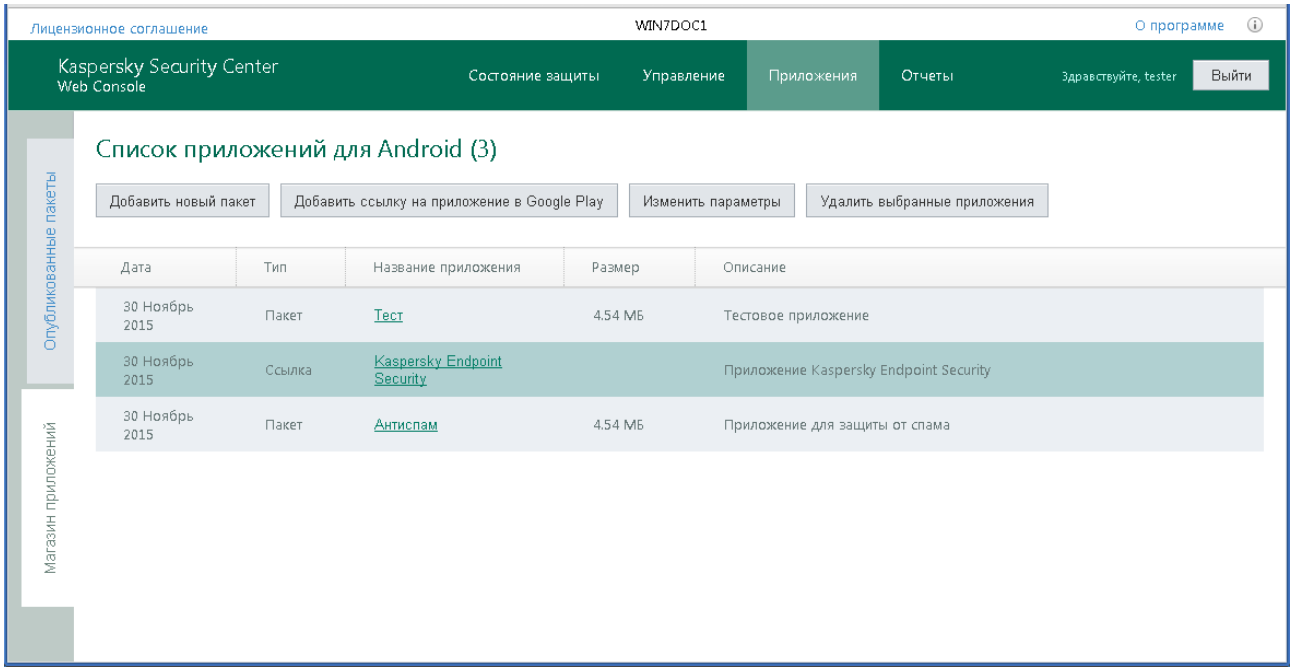

Рисунок 10. Главное окно программы Kaspersky Security Center Web Console

Просмотр магазина приложений

► *Чтобы просмотреть список приложений для Android в магазине приложений, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

На закладке **Магазин приложений** содержится список приложений для Android, добавленных в магазин (apk-файлы и ссылки на приложения в Google Play).

Список содержит следующую информацию о приложениях для Android:

- **Дата**. Дата добавления в список пакета или ссылки на приложение.
- **Тип**. Тип добавленного приложения: **Пакет** или **Ссылка**.
- **Название приложения**. Название приложения является ссылкой. По ссылке на приложение типа **Пакет**, Kaspersky Security Center Web Console загружает файл приложения на компьютер, на котором вы работаете в данный момент. По ссылке на приложение типа **Ссылка**, Kaspersky Security Center Web Console переходит на страницу этого приложения в Google Play.
- **Размер**. Размер пакета в мегабайтах. Указывается только для типа приложения **Пакет**.
- **Описание**. Описание приложения.

Изменение параметров приложения и удаление приложения из магазина

► *Чтобы изменить параметры приложения в магазине приложений, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.

3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.

4. Выберите приложение в списке и нажмите на кнопку **Изменить параметры** над списком.

   Если вы выбрали в списке приложение типа **Пакет**, откроется окно **Пакет с приложениями**. В этом окне вы можете выбрать apk-файл приложения, изменить название и описание приложения.

   Если вы выбрали в списке приложение типа **Ссылка**, откроется окно **Ссылка на приложение в Google Play**. В этом окне вы можете указать ссылку на приложение, изменить название и описание приложения.

5. Внесите необходимые изменения и нажмите на кнопку **Применить**.

В результате измененные параметры приложения будут отражены в магазине приложений.

► *Чтобы удалить приложение из магазина приложений, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.

4. Выберите приложение в списке.

   Вы можете выбрать несколько приложений в списке.

5. Нажмите на кнопку **Удалить выбранные приложения** над списком.

   Отобразится окно **Удаление**.

6. Нажмите на кнопку **Удалить**.

В результате выбранное приложение будет удалено из магазина.

Установка приложений из магазина приложений

► *Чтобы установить приложение из магазина приложений на Android-устройство с помощью apk-файла, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.
4. Выберите в списке приложение типа **Пакет**.
5. По ссылке с названием приложения загрузите apk-файл из магазина приложений на компьютер, на котором вы в данный момент работаете.
6. Перенесите apk-файл с компьютера на Android-устройство любым удобным для вас способом.
7. Запустите на устройстве установку приложения из apk-файла.

Для установки приложения в параметрах устройства должна быть разрешена установка приложений из неизвестных источников. Установка приложения из apk-файла выполняется обычным способом, принятым для устройств под управлением Android.

► *Чтобы установить приложение с помощью ссылки Google Play, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Приложения**.
3. Выберите закладку **Магазин приложений** в левой части окна.

   Отобразится **Список приложений для Android**.

4. Выберите в списке приложение типа **Ссылка**.
5. По ссылке с названием приложения откройте страницу приложения на Google Play.

   Страница приложения на Google Play открывается на новой вкладке браузера.
6. Нажмите на кнопку **Установить** на странице приложения.

Приложение запросит разрешение на установку. Установка приложения с Google Play будет выполнена обычным способом, принятым для устройств под управлением Android.

Управление политиками

Политика – это набор параметров работы программы, назначенный 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 создано несколько политик с различными значениями параметров, но активная политика для программы может быть только одна. Предусмотрена возможность активировать политику, не являющуюся активной, при наступлении определенного события. Это позволяет, например, устанавливать более жесткие параметры антивирусной защиты в периоды вирусных эпидемий.

Для разных групп администрирования 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

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. 15).
2. Выберите закладку **Управление**.
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).

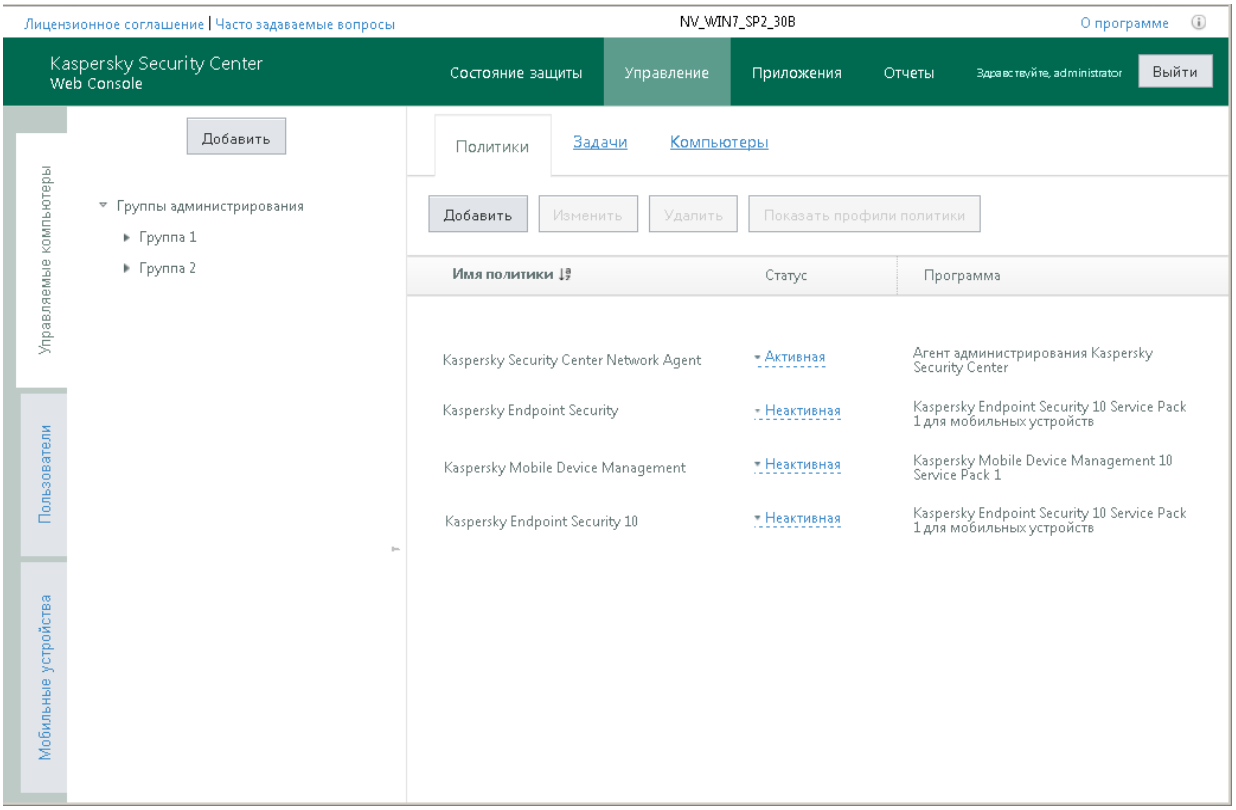

Рисунок 11. Просмотр списка политик

Список политик содержит следующую информацию о политиках:

- имя политики;
- статус политики (активная, неактивная, для автономных пользователей);
- название 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.

Добавление политики

► *Чтобы добавить политику, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Управляемые компьютеры**.
4. В разделе **Управляемые компьютеры** выберите закладку **Политики**.
5. В левой части окна выберите группу администрирования, для которой вы хотите добавить политику.
6. Нажмите на кнопку **Добавить**.

   Откроется окно мастера создания политики с приветственной надписью.
7. Нажмите на кнопку **Создать политику**.

8. В окне мастера **Выбор программы для создания групповой политики** выберите программу, для которой вы хотите создать политику и нажмите на кнопку **Вперед**.

   Откроется окно для ввода названия новой групповой политики.

9. В поле **Имя политики** введите название создаваемой групповой политики.

10. Нажмите на кнопку **Запустить** для завершения работы мастера создания политики.

Новая политика, созданная в результате работы мастера, будет добавлена в список политик на закладке **Политики** (см. раздел «**Просмотр списка политик**» на стр. 53). По умолчанию созданной политике назначается статус *Неактивная*. Вы можете изменить статус политики в графе **Статус** списка политик.

Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых программа не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Вы можете изменять политику после ее создания.

Параметры программ «Лаборатории Касперского», которые изменяются после применения политик, подробно описаны в Руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен «замок» ), начинают действовать на клиентских компьютерах независимо от того, какие параметры были настроены для программы ранее.

Управление профилями политик

Этот раздел содержит информацию о *профилях политик*, которые используются для эффективного управления группами клиентских компьютеров и мобильных устройств. Описаны преимущества профилей политик, способы их применения.

В этом разделе

О профиле политики

Профиль политики – это именованный набор переменных параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве) при выполнении определенных условий. При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик поддерживаются только для программ Kaspersky Endpoint Security 10 Service Pack 1 для Windows и Kaspersky Mobile Device Management 10 Service Pack 1.

Преимущества профилей политик

Профили политик облегчают управление клиентскими устройствами с помощью политик:

- Профили содержат только те параметры, которые отличаются от «базовой» политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.
- Новые профили политики удобно создавать, так как поддерживаются экспорт и импорт профилей, а также создание новых профилей на основе существующих с помощью копирования.
- На одном клиентском устройстве могут быть активны несколько профилей политики одновременно.
- Поддерживается иерархия политик.

Правила активации профиля. Приоритеты профилей

Профиль политики активируется на клиентском устройстве при выполнении правила активации. Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство размещено в определенном подразделении Active Directory®, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center Web Console.

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль *X* находится перед профилем *Y* в списке профилей, то профиль *X* имеет более высокий приоритет, чем *Y*. Приоритеты профилей необходимы, так как на клиентском устройстве одновременно может быть активно несколько профилей.

Политики в иерархии групп администрирования

В то время как политики влияют друг на друга в соответствии с иерархией групп администрирования, профили с одинаковыми именами объединяются. Профили более «высокой» политики имеют более высокий приоритет. Например, в группе администрирования *A* политика *P(A)* имеет профили *X1*, *X2*, и *X3*, в порядке убывания приоритета. В группе администрирования *B*, которая является подгруппой группы *A*, создана политика *P(B)*, с профилями *X2*, *X4*, *X5*. Тогда политика *P(B)* будет изменена политикой *P(A)*, так, что в политике *P(B)* список профилей в порядке убывания приоритета будет *X1*, *X2*, *X3*, *X4*, *X5*. Приоритет профиля *X2* будет зависеть от начального состояния *X2* политики *P(B)* и *X2* политики *P(A)*.

Активная политика является суммой главной политики и всех активных профилей этой политики, то есть тех профилей, для которых выполняются правила активации. Активная политика повторно вычисляется при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству.

Свойства и ограничения профиля политики

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если политика активна в автономном режиме, то и профили этой политики применяются только в автономном режиме.
- Профили не поддерживают статический анализ доступа к исполняемым файлам.
- Политика не может содержать параметры уведомлений.
- Если используется UDP порт 15000 для подключения клиентского компьютера к Серверу администрирования, то при назначении тега клиентскому компьютеру соответствующий профиль политики должен активироваться в течение одной минуты.
- Правила подключения Агента администрирования к Серверу администрирования можно использовать при создании правил активации профиля.

Добавление профиля политики

► *Чтобы добавить профиль политики, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Управляемые компьютеры**.
4. В разделе **Управляемые компьютеры** выберите закладку **Политики**.
5. В левой части окна выберите группу администрирования.
6. В списке политик выберите политику, для которой вы хотите добавить профиль.

7. Нажмите на кнопку **Показать профили политики**.

   Откроется список профилей политики.

8. Нажмите на кнопку **Добавить**.

   Откроется окно мастера создания профиля политики с приветственной надписью.

9. Нажмите на кнопку **Создать профиль политики**.

   Откроется окно для ввода параметров профиля политики.

10. В верхнем поле ввода укажите имя профиля политики. Имя профиля не может превышать 100 символов.

11. В списке **Правила активации** нажмите на кнопку **Добавить**, чтобы создать правило, по которому будет активирован профиль политики.

12. Установите флажок **Включить профиль**, чтобы профиль политики использовался клиентскими компьютерами или управляемыми устройствами.

13. Нажмите на кнопку **Запустить** для завершения работы мастера создания профиля политики.

Новый профиль политики, созданный в результате работы мастера, будет добавлен в список профилей политики. Список профилей политики вы можете посмотреть на закладке **Политики** по кнопке **Показать профили политики**. Параметры политики созданного профиля вы можете настроить на закладке **Политики** по кнопке **Изменить** (см. раздел «**Изменение профиля политики**» на стр. 59).

Изменение профиля политики

Вы можете изменять параметры профиля политики для программ «Лаборатории Касперского» после его создания.

► *Чтобы изменить профиль политики, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. В левой части окна выберите группу администрирования.

4. В списке политик выберите политику, для которой вы хотите изменить параметры профиля.
5. Нажмите на кнопку **Показать профили политики**.

   В нижней части окна откроется список профилей политики.
6. Выберите профиль, параметры которого вы хотите изменить.
7. Нажмите на кнопку **Изменить**.

   На экране откроется окно свойств групповой политики.
8. Настройте параметры профиля политики и параметры работы программы «Лаборатории Касперского» в соответствующих разделах.

   > Параметры программ «Лаборатории Касперского» подробно описаны в Руководствах для этих программ.
9. Нажмите на кнопку **ОК** для завершения изменения параметров профиля.

Измененные параметры начнут действовать после синхронизации клиентского компьютера или управляемого устройства с Сервером администрирования (если профиль политики активен), либо после выполнения правила активации (если профиль политики неактивен).

Активация политики

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

1. В главном окне программы (см. раздел «Интерфейс программы» на стр. 15) на закладке **Управление** 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.

Изменение политики

Вы можете изменять параметры групповых политик для программ «Лаборатории Касперского» после их создания.

► *Чтобы изменить политику, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Управляемые компьютеры**.
4. В разделе **Управляемые компьютеры** выберите закладку **Политики**.
5. В левой части окна выберите группу администрирования, для которой вы хотите изменить политику.
6. В списке политик выберите политику, параметры которой вы хотите изменить.
7. Нажмите на кнопку **Изменить**.

   На экране откроется окно свойств групповой политики.
8. Настройте параметры работы программы «Лаборатории Касперского».

   Параметры программ «Лаборатории Касперского» подробно описаны в Руководствах для этих программ.
9. Нажмите на кнопку **ОК** для завершения изменения параметров политики. Для применения параметров нажмите на кнопку **Применить**. Чтобы прекратить изменение политики, нажмите на кнопку **Отмена**. В этом случае изменения параметров политики не сохранятся.

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. 15) на закладке **Управление** 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. 15) на закладке **Управление** 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 мобильными устройствами с помощью MDM-политики

В разделе приведена информация об особенностях работы с политикой для программы Kaspersky Mobile Device Management 10 Service Pack 1.

В этом разделе

О MDM-политике

Для управления iOS MDM и EAS-устройствами (EAS-устройства подключаются к Серверу администрирования по протоколу Exchange ActiveSync®) вы можете использовать плагин управления Kaspersky Mobile Device Management 10 Service Pack 1, входящий в комплект поставки Kaspersky Security Center. Kaspersky Mobile Device Management позволяет создавать групповые политики для настройки конфигурационных параметров iOS MDM и EAS-устройств. Групповая политика, позволяющая просматривать и настраивать конфигурационные параметры iOS MDM и EAS-устройств, называется MDM-политикой.

MDM-политика предоставляет администратору следующие возможности:

- для управления EAS-устройствами:
  - настраивать параметры пароля для разблокирования устройства;
  - настраивать хранение данных на устройстве в зашифрованном виде;
  - настраивать параметры синхронизации корпоративной почты;
  - настраивать аппаратные функции мобильных устройств, например, использование съемных дисков, использование камеры, использование Bluetooth;
  - настраивать ограничения для использования мобильных приложений на устройстве.

- для управления iOS MDM-устройствами:
  - настраивать параметры безопасности использования пароля на устройстве;
  - настраивать ограничения для использования аппаратных функций устройства, а также ограничения на установку и удаление мобильных приложений;
  - настраивать ограничения для использования на устройстве встроенных мобильных приложений, например, YouTube™, iTunes Store, Safari;
  - настраивать ограничения просмотра медиаконтента (например, фильмов и тв-шоу) по региону местоположения устройства;
  - настраивать параметры подключения устройства к интернету через прокси-сервер (Глобальный HTTP-прокси);
  - настраивать параметры единой учетной записи, с помощью которой пользователь может получить доступ к корпоративным приложениям и сервисам (технология единого входа);
  - контролировать использование интернета (посещение веб-сайтов) на мобильных устройствах;
  - настраивать параметры беспроводных сетей (Wi-Fi), точек доступа (APN), виртуальных частных сетей (VPN) с использованием различных механизмов аутентификации и сетевых протоколов;
  - настраивать параметры подключения к устройствам AirPlay для потоковой передачи фотографий, музыки и видео;
  - настраивать параметры подключения к принтерам AirPrint для печати документов с устройства беспроводным способом;
  - настраивать параметры синхронизации с сервером Microsoft Exchange, а также учетные записи пользователей для использования корпоративной почты на устройствах;
  - настраивать учетные данные пользователя для синхронизации со службой каталогов LDAP;

- настраивать учетные данные пользователя для подключения к сервисам CalDAV и CardDAV, что позволяет пользователю использовать корпоративные календари и списки контактов;
- настраивать параметры интерфейса iOS на устройстве пользователя, например, шрифты или иконки для избранных веб-сайтов;
- добавлять новые сертификаты безопасности на устройство;
- настраивать параметры SCEP-сервера для автоматического получения устройством сертификатов из Центра сертификации;
- добавление собственных параметров для работы мобильных приложений.

Общие принципы работы MDM-политики не отличаются от принципов работы политик, созданных для управления другими программами. Особенностью MDM-политики является то, что она назначается на группу администрирования, в которую входят Сервер мобильных устройств iOS MDM и Сервер мобильных устройств Exchange Active Sync (далее серверы мобильных устройств). Все параметры, заданные в MDM-политике, сначала распространяются на серверы мобильных устройств, затем на мобильные устройства, которыми они управляют. В случае использования иерархической структуры групп администрирования подчиненные серверы мобильных устройств получают параметры MDM-политики с главных серверов мобильных устройств и распространяют их на мобильные устройства.

Подробные сведения о работе с MDM-политикой в Консоли администрирования Kaspersky Security Center см. в Руководстве администратора по комплексному решению Kaspersky Security для мобильных устройств.

Настройка параметров MDM-политики

С помощью MDM-политики вы можете настраивать конфигурационные параметры EAS-устройств и iOS MDM-устройств. Параметры EAS-устройств можно задать в окне свойств MDM-политики в разделе **Параметры EAS-устройств**. Параметры iOS MDM-устройств вы можете настроить с помощью сторонних утилит iPhone Configuration Utility или Apple Configurator, а затем импортировать настроенные параметры в MDM-политику. С помощью утилит iPhone Configuration Utility или Apple Configurator вы также можете экспортировать параметры iOS MDM-устройств в файл для просмотра и изменения.

► *Чтобы импортировать конфигурационные параметры iOS MDM-устройств из файла, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Управляемые компьютеры**.
4. В разделе **Управляемые компьютеры** выберите закладку **Политики**.
5. В левой части окна выберите группу администрирования, для которой вы хотите импортировать MDM-политику.
6. В списке политик выберите MDM-политику, параметры которой вы хотите импортировать.
7. Нажмите на кнопку **Изменить**.

   Откроется окно свойств MDM-политики.
8. В окне свойств MDM-политики выберите закладку **Экспорт / Импорт параметров**.
9. Нажмите на кнопку **Импортировать**.
10. В открывшемся окне выберите файл с расширением `mobileconfig`.

В результате будет выполнен импорт конфигурационных параметров iOS MDM-устройств из выбранного файла в MDM-политику.

► *Чтобы экспортировать конфигурационные параметры iOS MDM-устройств в файл, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Управляемые компьютеры**.
4. В разделе **Управляемые компьютеры** выберите закладку **Политики**.

5. В левой части окна выберите группу администрирования, для которой вы хотите экспортировать MDM-политику.
6. В списке политик выберите MDM-политику, параметры которой вы хотите экспортировать.
7. Нажмите на кнопку **Изменить**.

   Откроется окно свойств MDM-политики.
8. В окне свойств MDM-политики выберите закладку **Экспорт / Импорт параметров**.
9. Нажмите на кнопку **Экспортировать**.

В результате будет выполнен экспорт конфигурационных параметров iOS MDM-устройств в файл с расширением `mobileconfg`. Вы можете открыть этот файл с помощью iPhone Configuration Utility или Apple Configurator.

Управление учетными записями пользователей

Kaspersky Security Center Web Console позволяет управлять учетными записями пользователей и групп пользователей. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей. Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center Web Console.

Все учетные записи пользователей можно просмотреть в разделе **Пользователи** (см. стр. 69).

Вы можете выполнять с учетными записями пользователей и групп пользователей следующие действия:

- фильтровать список учетных записей (см. стр. 70);
- просматривать данные о пользователе (см. стр. 71);
- просматривать список мобильных устройств пользователя (см. стр. 72).

В этом разделе

Просмотр списка учетных записей

При работе с учетными записями вы можете просмотреть список учетных записей пользователей, а также групп пользователей, созданных на Сервере администрирования.

► *Чтобы просмотреть список учетных записей, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Пользователи**.

   В разделе **Пользователи** отображается список учетных записей пользователей (см. рис. ниже). По умолчанию список учетных записей содержит следующую информацию о пользователях:

   - Значок типа учетной записи. Если значок имеет вид , учетная запись создана для одного пользователя. Если значок имеет вид , то учетная запись создана для группы пользователей.

   - Имя пользователя. Имя учетной записи или имя группы учетных записей.

   Вы можете добавлять в список графы с дополнительной информацией об учетной записи по кнопке **Показать данные о пользователе**.

4. Просмотрите список учетных записей, используя следующие элементы интерфейса:

   - кнопки |< < > >| – переход к следующей / предыдущей, первой / последней странице списка учетных записей;

- значок в заголовке графы – сортировка учетных записей в списке в алфавитном порядке.

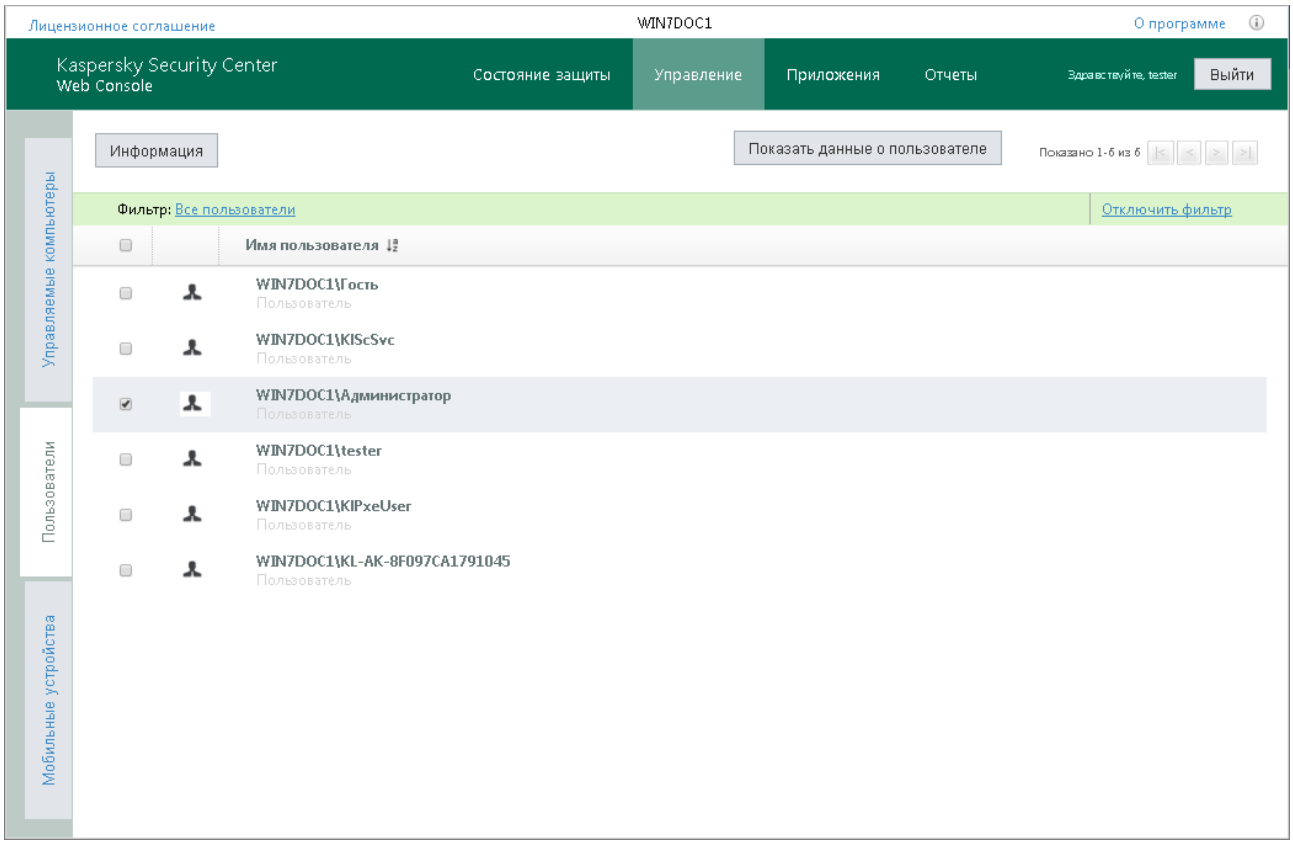

Рисунок 12. Список учетных записей пользователей

Фильтрация списка учетных записей

Для удобства работы со списком учетных записей вы можете отфильтровать его по заданным параметрам.

► *Чтобы отфильтровать список учетных записей, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. на закладке **Управление** выберите раздел **Пользователи**.

   На экране отобразится список учетных записей пользователей.

4. По ссылке рядом с надписью **Фильтр** в верхней части окна откройте окно настройки фильтра.

5. В открывшемся окне **Фильтр: Пользователи** настройте фильтрацию списка учетных записей:

   - По заданному тексту, содержащемуся в данных учетной записи.
   - По данным учетной записи, таким как имя, тип пользователя, название организации, адрес электронной почты и прочее.

6. Нажмите на кнопку **ОК**, чтобы отфильтровать список учетных записей.

Отменить фильтрацию списка учетных записей пользователей вы можете по ссылке **Отключить фильтр** в верхней части раздела **Пользователи**.

Просмотр данных о пользователе

► *Чтобы просмотреть данные о пользователе, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Пользователи**.

   В разделе **Пользователи** отображается список учетных записей пользователей.

4. В списке выберите учетную запись пользователя или группы пользователей, информацию о которой вы хотите посмотреть.

5. В верхней части раздела нажмите на кнопку **Информация**.

6. В открывшемся окне **Информация о пользователе** выберите раздел **Данные пользователя**.

На экране отобразятся данные о пользователе (см. рис. ниже).

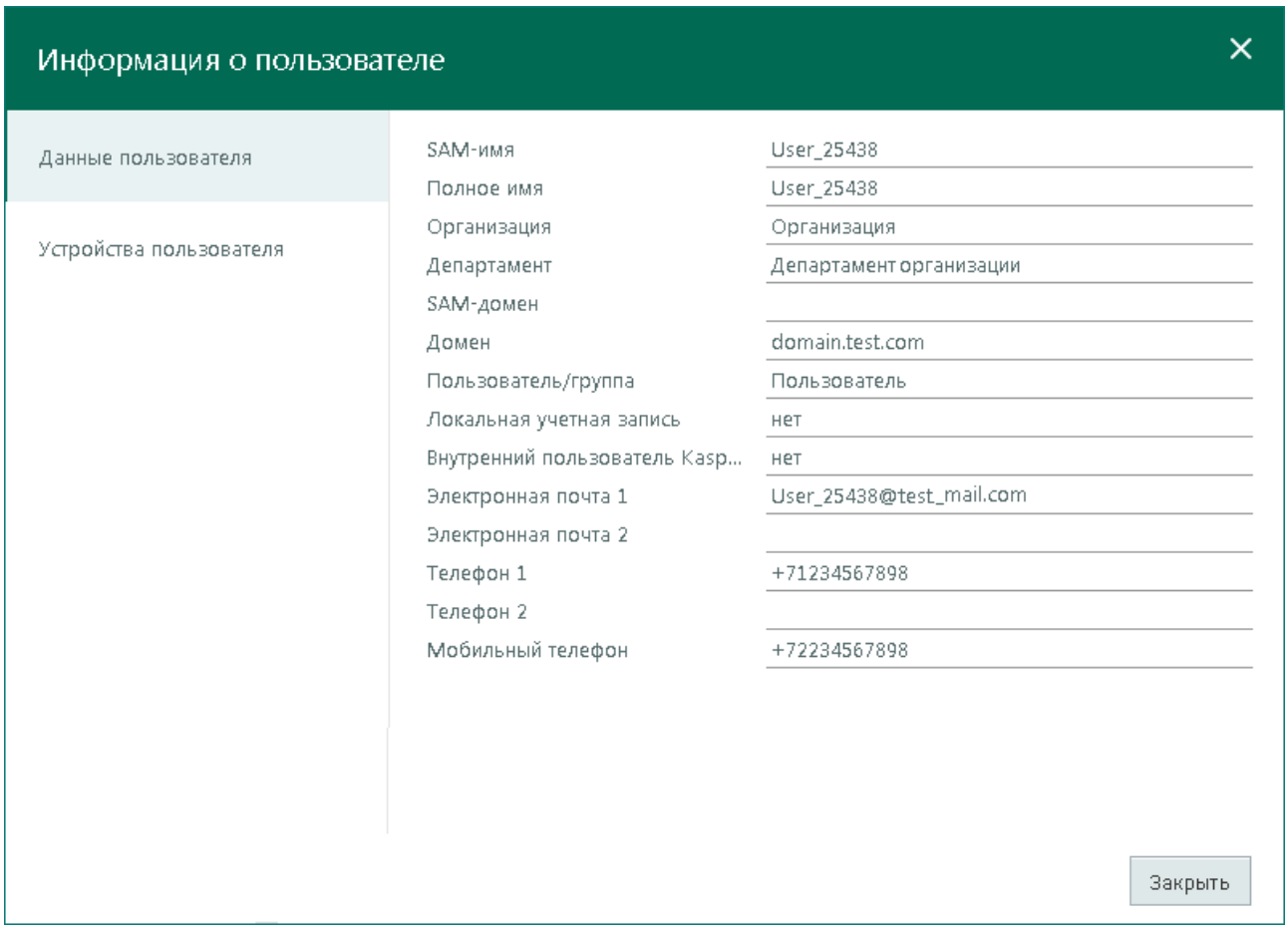

Рисунок 13. Данные учетной записи пользователя

Просмотр списка мобильных устройств пользователя

► *Чтобы посмотреть список мобильных устройств пользователей, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Пользователи**.

   На экране отобразится список учетных записей пользователей.

4. В списке выберите учетную запись пользователя, список мобильных устройств которого вы хотите посмотреть.

5. В верхней части раздела нажмите на кнопку **Информация**.

6. В открывшемся окне **Информация о пользователе** выберите раздел **Устройства пользователя**.

   На экране отобразится список мобильных устройств пользователя, подключенных к Серверу администрирования (см. рис ниже).

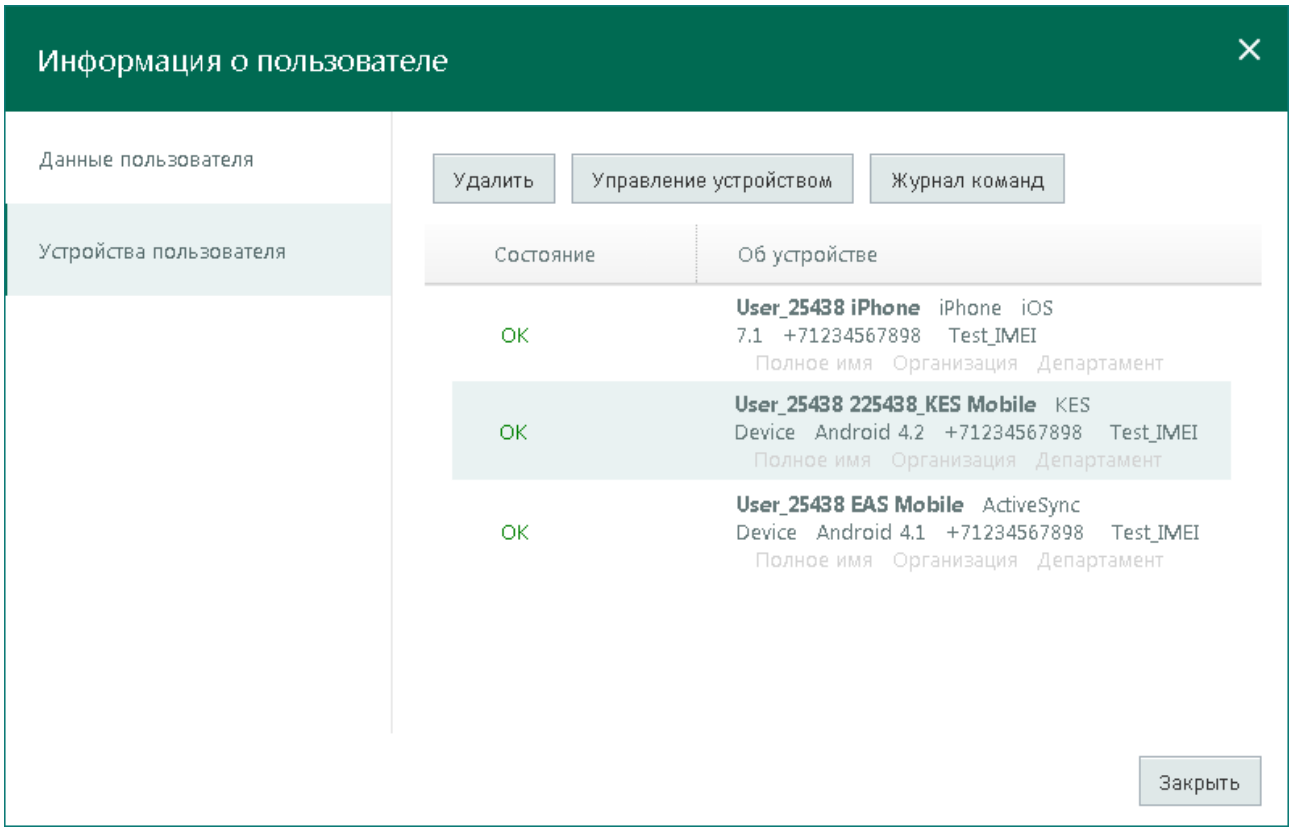

Рисунок 14. Список мобильных устройств пользователя

В разделе **Устройства пользователя** вы можете не только посмотреть информацию о каждом устройстве пользователя, но и отправить на выбранное устройство команду, отследить статус выполнения команды в журнале команд, а также удалить устройство из списка.

Управление мобильными устройствами

Kaspersky Security Center Web Console позволяет управлять мобильными устройствами пользователей, подключенными к Серверу администрирования Kaspersky Security Center. Такие мобильные устройства называются *управляемыми мобильными устройствами*.

Список всех управляемых мобильных устройств отображается в разделе **Мобильные устройства** на закладке **Управление** главного окна программы.

Вы можете выполнять с мобильными устройствами пользователей следующие действия:

- просматривать информацию о мобильном устройстве (см. стр. 76);
- просматривать информацию о владельце мобильного устройства (см. стр. 77);
- отправлять команды на мобильное устройство (см. стр. 81);
- просматривать журнал выполнения команд (см. стр. 82);
- удалять мобильные устройства из списка (см. стр. 82).

В этом разделе

Просмотр списка мобильных устройств

Вы можете просмотреть список всех мобильных устройств, управляемых Сервером администрирования.

► *Чтобы просмотреть список мобильных устройств, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Мобильные устройства**.

   В разделе **Мобильные устройства** отображается список управляемых мобильных устройств (см. рис ниже). По умолчанию список содержит следующую информацию об устройствах:

   - **Состояние**. Информация о статусе подключения и работе мобильного устройства.

   - **Об устройстве**. Общая информация об устройстве: имя мобильного устройства в Kaspersky Security Center, название организации и департамента, название и версия операционной системы, номер телефона.

4. Просмотрите список мобильных устройств, используя кнопки  для перехода к следующей / предыдущей, первой / последней странице списка мобильных устройств.

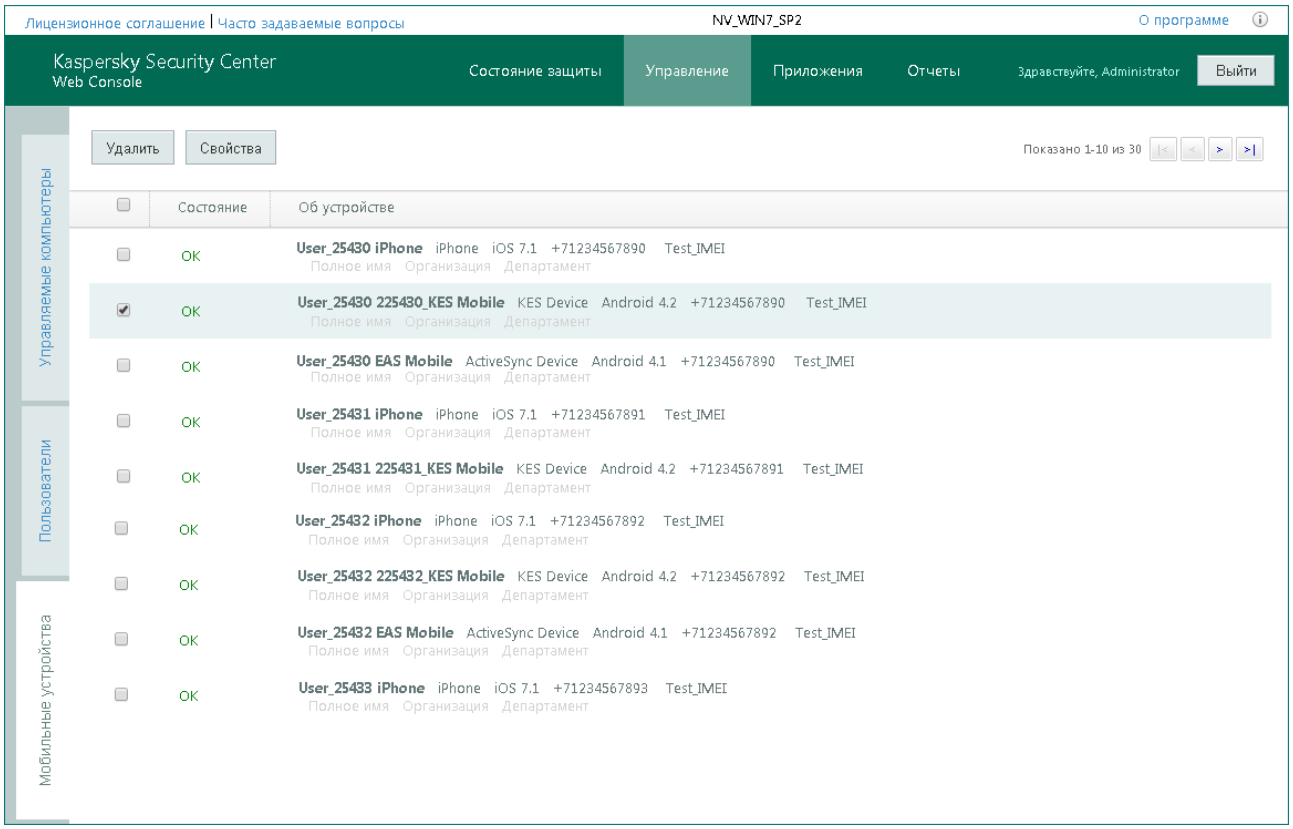

Рисунок 15. Список управляемых мобильных устройств

Просмотр параметров мобильного устройства

► *Чтобы посмотреть параметры мобильного устройства, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Мобильные устройства**.

   В разделе **Мобильные устройства** отображается список управляемых мобильных устройств.

4. В списке выберите мобильное устройство, параметры которого вы хотите посмотреть.

5. В верхней части раздела нажмите на кнопку **Свойства**.

6. В открывшемся окне **Информация об устройстве** выберите раздел **Данные устройства**.

На экране отобразится информация о мобильном устройстве (версия операционной системы, модель, номер телефона SIM-карты и прочее).

Если вы хотите посмотреть параметры, необходимые для работы протокола, под управлением которого находится устройство, выберите раздел **Параметры <название протокола>**, или **Дополнительные параметры <название протокола>**, или **Kaspersky Endpoint Security**.

Просмотр информации о владельце устройства

► *Чтобы посмотреть информацию о пользователе мобильного устройства, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).

2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Мобильные устройства**.

   В разделе **Мобильные устройства** отображается список управляемых мобильных устройств.

4. Выберите в списке мобильное устройство, информацию о котором вы хотите посмотреть.

5. В верхней части раздела нажмите на кнопку **Свойства**.

6. В открывшемся окне **Информация об устройстве** выберите раздел **Владелец**.

На экране отобразятся сведения об учетной записи пользователя, под именем которой мобильное устройство подключено к Серверу администрирования (полное имя учетной записи, название организации, домен учетной записи, адрес электронной почты и прочее).

Команды для управления мобильными устройствами

Kaspersky Security Center Web Console поддерживает команды для управления мобильными устройствами.

Команды используются для дистанционного управления мобильными устройствами. Например, в случае потери мобильного устройства, с помощью команды можно удалить корпоративные данные с устройства.

Вы можете использовать команды для следующих типов управляемых мобильных устройств:

- iOS MDM-устройства;
- KES-устройства;
- EAS-устройства.

Каждый тип устройства поддерживает свой набор команд. В таблице ниже приведен список команд для каждого типа устройства.

Для всех типов устройств в случае успешного выполнения команды **Удалить данные**, все данные будут удалены с устройства, настройки устройства будут сброшены до заводских.

Для iOS MDM-устройства в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.

Для KES-устройства в случае успешного выполнения команды **Удалить корпоративные данные** с устройства будут удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google™. Для KES-устройства дополнительно будут удалены данные с карты памяти.

Таблица 2. Список поддерживаемых команд

Тип мобильного устройства	Команды	Результат выполнения команды
iOS MDM-устройство	Заблокировать	Устройство заблокировано.
	Разблокировать	Выключена блокировка устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Полная очистка	Удалены все данные с устройства, настройки устройства сброшены до заводских.
	Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
KES-устройство	Разблокировать	Выключена блокировка устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Полная очистка	Удалены все данные с устройства, настройки устройства сброшены до заводских.

Тип мобильного устройства	Команды	Результат выполнения команды
	Удалить корпоративные данные	Удалены корпоративные данные, записи в Контактах, история SMS, журнал вызовов, календарь, параметры подключения к интернету, учетные записи пользователя, кроме учетной записи Google. Удалены данные с карты памяти.
	Определить местоположение	Устройство заблокировано. Местоположение устройства определено и показано на Google Картах™. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Сфотографировать	Устройство заблокировано. Фотография выполнена фронтальной камерой устройства и сохранена на Сервере администрирования. Фотографии доступны для просмотра в журнале команд. Оператор мобильной связи взимает оплату за передачу SMS и интернет.
	Воспроизвести звуковой сигнал	Устройство заблокировано. Устройство воспроизводит звуковой сигнал.
EAS-устройство	Полная очистка	Удалены все данные с устройства, настройки устройства сброшены до заводских.

Отправка команд на мобильное устройство

Вы можете дистанционно отправлять команды для управления мобильными устройствами.

► *Чтобы отправить команду на мобильное устройство, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. На закладке **Управление** выберите раздел **Мобильные устройства**.
4. В разделе **Мобильные устройства** отображается список управляемых мобильных устройств.
5. В списке выберите мобильное устройство, на которое вы хотите отправить команду.
6. В верхней части раздела нажмите на кнопку **Свойства**.
7. В открывшемся окне **Информация об устройстве** выберите раздел **Управление устройством**.
8. В списке команд выберите команду, которую вы хотите выполнить на устройстве, и нажмите на кнопку с ее названием.

В зависимости от выбранной команды после нажатия на кнопку с ее названием может открыться дополнительное окно, в котором следует подтвердить отправку команды. Например, дополнительное окно открывается для команды **Удаление корпоративных данных**, поскольку выполнение этой команды приводит к потере данных на мобильном устройстве.

Просмотр журнала команд

► *Чтобы просмотреть журнал команд, отправленных на мобильное устройство, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.
3. В открывшемся окне выберите раздел **Мобильные устройства**.

   В разделе **Мобильные устройства** отображается список управляемых мобильных устройств.
4. Выберите в списке мобильное устройство, для которого вы хотите просмотреть журнал команд.
5. В верхней части раздела нажмите на кнопку **Свойства**.
6. В открывшемся окне **Информация об устройстве** выберите раздел **Журнал выполнения команд**.

   На экране отобразится список команд, отправленных на устройство. Журнал выполнения команд содержит информацию о каждой команде, отправленной на устройство:

   - **Дата Время**. Информация о дате и времени отправки команды на устройство.
   - **Название Статус**. Название команды и статус ее выполнения.

Удаление мобильного устройства из списка

► *Чтобы удалить мобильное устройство из списка, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Управление**.

3. На закладке **Управление** выберите раздел **Мобильные устройства**.

   На экране отобразится список управляемых мобильных устройств.

4. Установите флажок напротив мобильного устройства, которое вы хотите удалить из списка.

   Вы можете выбрать несколько мобильных устройств.

5. В верней части раздела нажмите на кнопку **Удалить**.

6. В открывшемся окне **Удаление** подтвердите удаление устройства из списка, нажав на кнопку **Удалить**.

В результате выбранное мобильное устройство будет удалено из списка и отключено от управления Сервером администрирования.

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

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. 15).
2. Выберите закладку **Управление**.

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).

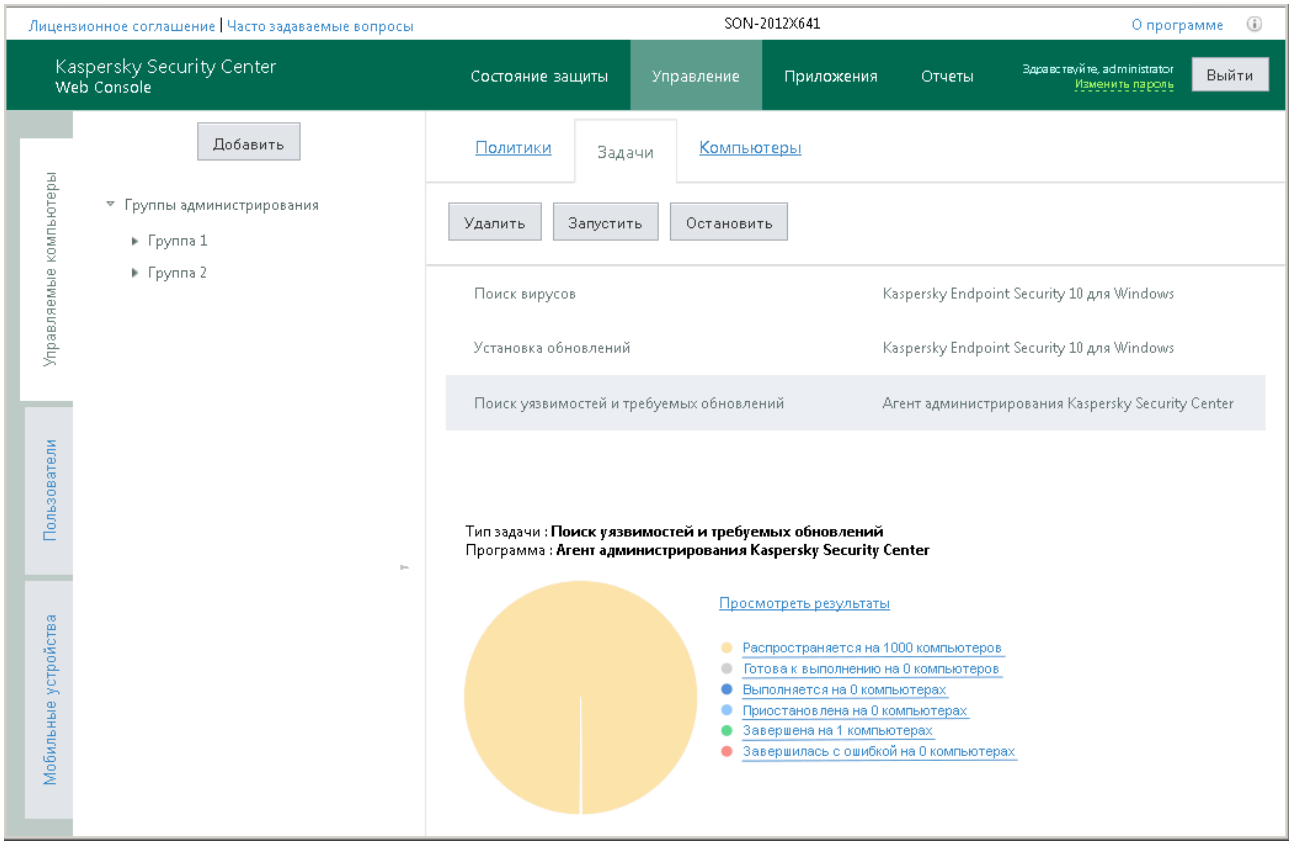

Рисунок 16. Просмотр списка задач

Список задач содержит следующую информацию о задачах:

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

В нижней части окна отображается статистка 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. 15) на закладке **Управление** 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. 15) на закладке **Управление** 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. 15) на закладке **Управление** 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

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 адресов электронной почты 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

► *Чтобы просмотреть отчет, выполните следующие действия:*

1. Откройте главное окно программы (см. раздел «Интерфейс программы» на стр. 15).
2. Выберите закладку **Отчеты**.
3. В списке отчетов в левой части окна выберите отчет, который вы хотите просмотреть (см. рис. ниже).

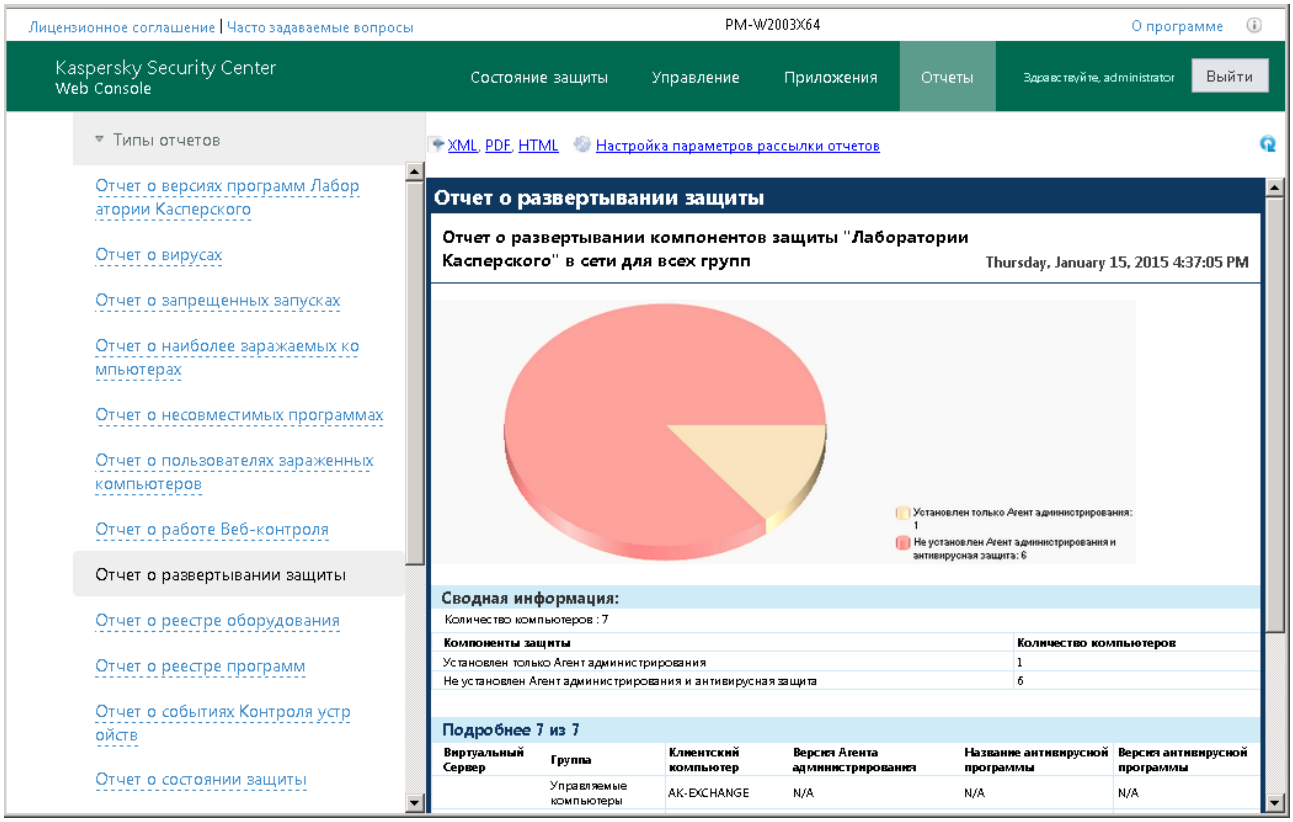

Рисунок 17. Просмотр отчетов

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. 15).
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. 15).
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 **Enter**.

        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:
     a. Выберите в списке рассылки адрес электронной почты, который вы хотите изменить.

        Выбранный адрес электронной почты отобразится в поле **Адрес получателя**.
     b. Измените адрес электронной почты в поле **Адрес получателя** и нажмите на кнопку **Enter**.

        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. 15).
2. Перейдите по ссылке **Сменить пароль**, расположенной справа вверху, 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 браузера, не завершив сеанс работы (например, закрыв окно или вкладку браузера), то сеанс будет оставаться активным в течение 24 часов после выхода.

► *Чтобы завершить сеанс работы с Kaspersky Security Center Web Console,*

находясь в главном окне программы (см. раздел «Интерфейс программы» на стр. 15), нажмите на кнопку **Выйти**, расположенную в правом верхнем углу окна.

Сеанс работы с Kaspersky Security Center Web Console будет завершен. В браузере откроется окно ввода имени пользователя и пароля (см. раздел «Процесс подключения к Серверу администрирования» на стр. 18).

Глоссарий

E

EAS-устройство

Мобильное устройство, которое подключается к Серверу администрирования по протоколу Exchange ActiveSync. По протоколу Exchange ActiveSync могут подключаться и управляться устройства с операционными системами iOS, Android, Windows Phone®.

H

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.

I

iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу мобильных устройств iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

J

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 браузера надо включить поддержку JavaScript.

K

KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android

S

SSL

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

A

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 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 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.

М

Магазин приложений

Компонент программы Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать apk-файлы приложений и ссылки на приложения в Google Play.

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.

АО «Лаборатория Касперского»

«Лаборатория Касперского» – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от 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 конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). В России, по данным IDC, «Лаборатория Касперского» – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей («IDC Endpoint Tracker 2014»).

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

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

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера 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 тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами «Лаборатории Касперского».

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 программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

ДОСТИЖЕНИЯ. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.ru/
Вирусная лаборатория:	http://newvirus.kaspersky.ru (для проверки подозрительных файлов и веб-сайтов)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt. В Kaspersky Security Center Web Console информацию из файла legal_notices.txt вы можете посмотреть в окне **О программе** по ссылке **Информация о стороннем коде**.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Acrobat – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Android, Chrome, Google, Google Play, Google Карты, YouTube – товарные знаки Google, Inc.

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

AirPlay, AirPrint, Apple, iPhone, iTunes, Mac OS, OS X, Safari – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Firefox – товарный знак Mozilla Foundation.

JavaScript, Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

Предметный указатель

Г

И

К

О

П

С

У