Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Dr.Web CureNet!

для Windows

антивирус.рф
www.drweb.ru

Централизованное средство проверки и лечения рабочих станций и серверов Windows, в том числе с установленным антивирусом другого производителя, в локальных сетях любого масштаба

- В Реестре отечественного ПО
- Не зависит от подключения к Интернету
- Запуск с любых внешних носителей или с iPhone/iPod touch

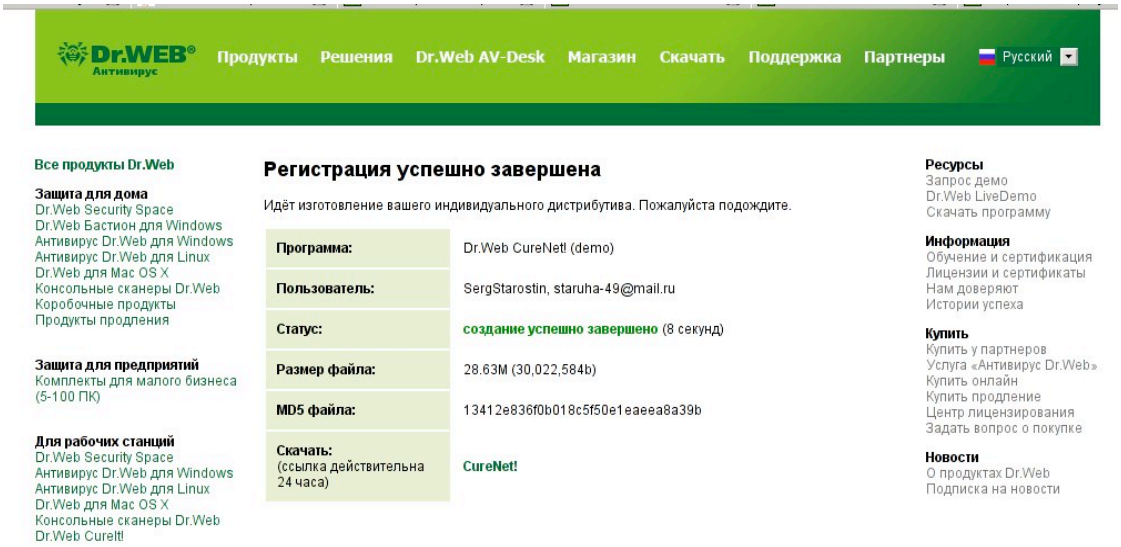
Краткое руководство по настройке и запуску Dr.Web CureNet!

Dr.Web CureNet! предназначен для проведения централизованной антивирусной проверки компьютеров по сети без установки антивируса на удаленные компьютеры. Dr.Web CureNet! позволяет проверять рабочие станции и серверы, работающие под управлением операционной системы Microsoft® Windows®, вне зависимости от устройства локальной сети, в которую они включены.

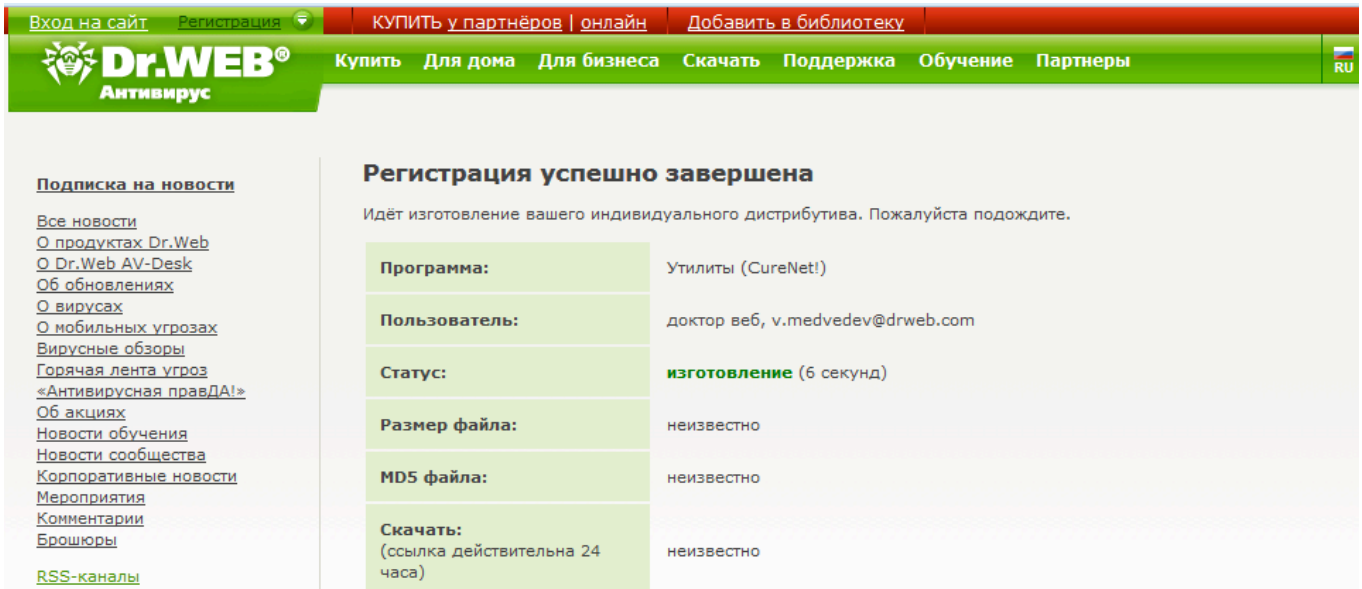
Внимание! Dr.Web CureNet! не предназначен для постоянной защиты локальной сети или отдельных компьютеров, так как в промежутках между проверками они могут заражаться вредоносными программами различных типов. Для организации надежной защиты компьютеров локальной сети рекомендуется использовать такие продукты, как Dr.Web Security Space или Dr.Web Enterprise Security Suite.

Получение дистрибутива Dr.Web CureNet!

Для того чтобы получить дистрибутив, необходимо зарегистрировать полученный серийный номер на странице http://products.drweb.com/register.



После завершения регистрации для вас будет автоматически сформирован индивидуальный дистрибутив продукта.



Созданный дистрибутив вы также можете скачать из своего личного кабинета. В дальнейшем, в течение срока действия лицензии из личного кабинета вы можете загружать свежие версии дистрибутива утилиты.

Переход в кабинет возможен как из самой из программы, так и после ввода серийного номера на странице http://support.drweb.com/get+cabinet+link.

Если серийный номер Dr.Web CureNet! уже был зарегистрирован, то вам просто нужно зайти в личный кабинет Dr.Web CureNet! и скачать актуальную версию дистрибутива.

Системные требования

Для удаленного сканирования компьютеров с использованием Dr.Web CureNet! необходимо соблюдение следующих требований:

- сканируемые компьютеры должны быть доступны по сети;
- учетная запись, используемая Dr.Web CureNet! для подключения к сканируемым компьютерам, должна существовать и обладать необходимыми административными привилегиями;
- порты 139 and 445 на сканируемых компьютерах должны быть открыты.

Для осуществления проверки антивирусной утилитой Dr.Web CureNet! вы должны иметь права администратора соответствующих рабочих станций и серверов. Удаленная проверка не требует дополнительной настройки компьютеров, если они входят в домен и на них используется доменная учетная запись администратора. В случае если удаленная машина не входит в домен или используется локальная учетная запись, то для ряда версий ОС Windows необходима дополнительная настройка удаленной машины. Подробные настройки ОС Windows описаны ниже. Вы также можете ознакомиться с обучающими видеоматериалами.

В связи с тем, что настройка для удаленной проверки может снизить безопасность удаленной машины, настоятельно рекомендуется ознакомиться с назначением указанных настроек перед внесением изменений в систему либо отказаться от использования удаленной проверки и провести антивирусную проверку непосредственно на удаленной машине вне домена или с использованием локальной учетной записи.

Настройка ОС Windows для запуска Мастера

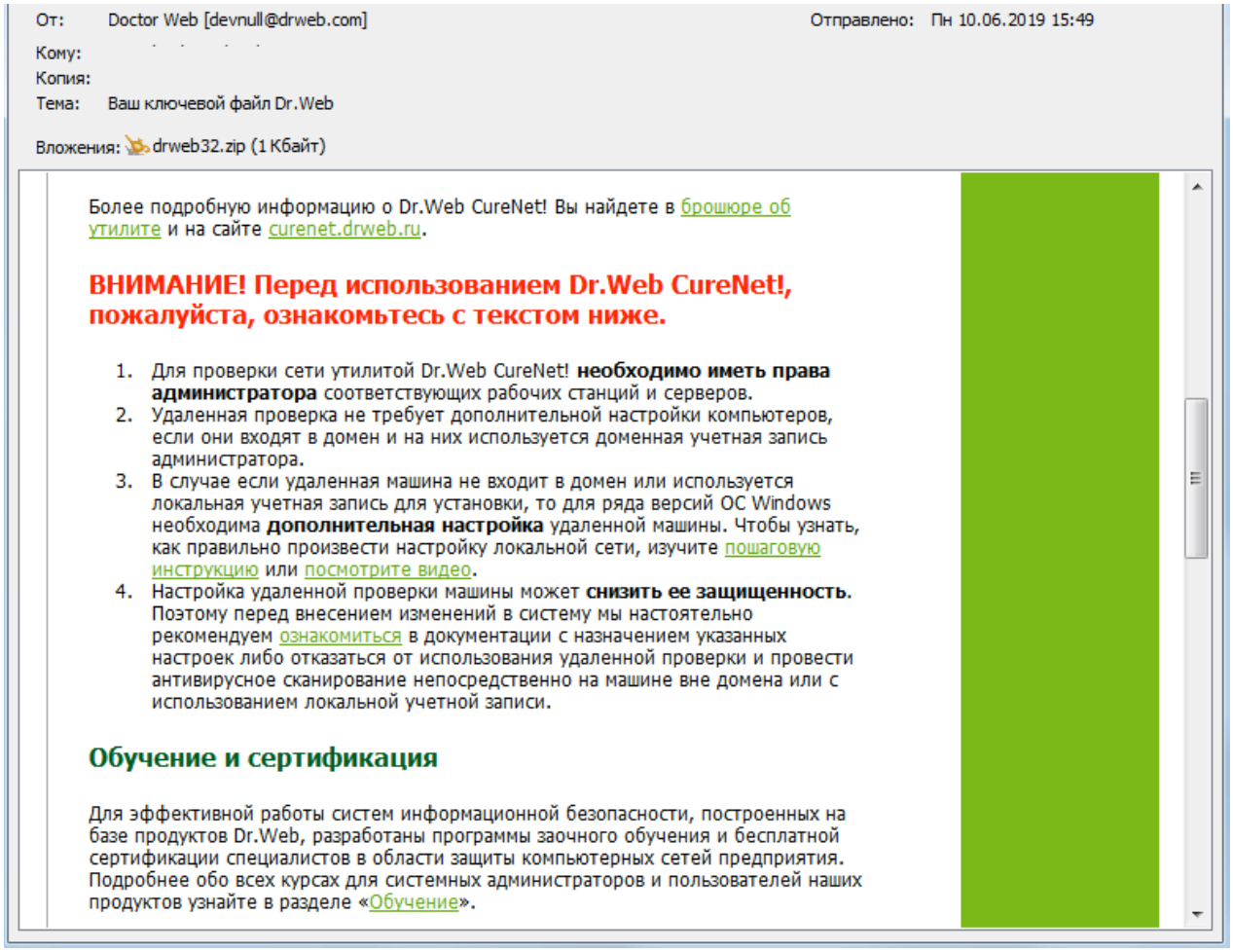
Мастер в составе дистрибутива Dr.Web CureNet! может функционировать в среде следующих версий ОС Windows:

- Windows XP (Professional с пакетом обновлений SP2 или более поздним)
- Windows Server 2003 с пакетом обновлений SP1 или более поздним
- Windows Vista (Business, Ultimate, Enterprise) с пакетом обновлений SP1 или более поздним
- Windows Server 2008
- Windows 7 (Профессиональная, Максимальная, Корпоративная)
- Windows Server 2008 R2
- Windows 8, Windows 8.1 (Профессиональная/Professional, Корпоративная/Enterprise)
- Windows Server 2012
- Windows 10

Для нормальной работы Мастера необходимо выполнение следующих условий.

1. Подключение к сети Интернет для обновления вирусных баз и компонентов Dr.Web.
2. Подключение ко всем проверяемым станциям по протоколу TCP/IP.

Краткая информация о требованиях по настройке OS Windows приводится в письме, которое направляется на электронный адрес, указанный при регистрации. Полные требования приведены в документации.



От: Doctor Web [devnull@drweb.com] Отправлено: Пн 10.06.2019 15:49
Кому:
Копия:
Тема: Ваш ключевой файл Dr.Web
Вложения: drweb32.zip (1 Кбайт)

Более подробную информацию о Dr.Web CureNet! Вы найдете в брошюре об утилите и на сайте curenet.drweb.ru.

ВНИМАНИЕ! Перед использованием Dr.Web CureNet!, пожалуйста, ознакомьтесь с текстом ниже.

1. Для проверки сети утилитой Dr.Web CureNet! **необходимо иметь права администратора** соответствующих рабочих станций и серверов.
2. Удаленная проверка не требует дополнительной настройки компьютеров, если они входят в домен и на них используется доменная учетная запись администратора.
3. В случае если удаленная машина не входит в домен или используется локальная учетная запись для установки, то для ряда версий ОС Windows необходима **дополнительная настройка** удаленной машины. Чтобы узнать, как правильно произвести настройку локальной сети, изучите пошаговую инструкцию или посмотрите видео.
4. Настройка удаленной проверки машины может **снизить ее защищенность**. Поэтому перед внесением изменений в систему мы настоятельно рекомендуем ознакомиться в документации с назначением указанных настроек либо отказаться от использования удаленной проверки и провести антивирусное сканирование непосредственно на машине вне домена или с использованием локальной учетной записи.

Обучение и сертификация

Для эффективной работы систем информационной безопасности, построенных на базе продуктов Dr.Web, разработаны программы заочного обучения и бесплатной сертификации специалистов в области защиты компьютерных сетей предприятия. Подробнее обо всех курсах для системных администраторов и пользователей наших продуктов узнайте в разделе «Обучение».

Настройка ОС Windows для удаленного запуска сканера Dr.Web

Общие настройки для Windows XP — 10, Windows Server 2003/2008/2012

Системные требования для станций совпадают с требованиями для компьютера, на котором запускается Мастер, за исключением списка поддерживаемых ОС: Windows XP Professional SP2 и более поздние версии, кроме следующих версий для 64-разрядных систем: Windows Server 2003 x64 Edition и Windows XP Professional SP2 x64 Edition.

- **Windows XP**

  Поддерживаются редакции — Windows XP Professional. Windows XP должна содержать пакет обновления (Service Pack) 2 или 3.

  Загрузить пакет обновления 2 для Windows XP:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=28

  Загрузить пакет обновления 3 для Windows XP (рекомендуется):

  http://www.microsoft.com/ru-ru/download/details.aspx?id=24

  Не поддерживаются редакции:

  - Windows XP Starter
  - Windows XP Home Edition

- **Windows 2003**

  Система Windows 2003 должна содержать пакет обновления 1 или 2.

  Загрузить пакет обновления 1 для Windows 2003:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=11435

  Загрузить пакет обновления 2 для Windows 2003 (рекомендуется):

  http://www.microsoft.com/ru-ru/download/details.aspx?id=41

- **Windows Vista**

  Система должна содержать пакет обновления 1 или 2.

  Поддерживаются редакции:

  - Windows Vista Business
  - Windows Vista Enterprise
  - Windows Vista Ultimate

  Не поддерживаются редакции:

  - Windows Vista Starter
  - Windows Vista Home Basic
  - Windows Vista Home Premium

  Загрузить пакет обновления 1 для Windows Vista:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=910

  Загрузить пакет обновления 2 для Windows Vista (рекомендуется):

  http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

- **Windows Server 2008**

  Система должна содержать пакет обновления 2.

  Загрузить пакет обновления 2 для Windows Server 2008:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

- **Windows 7**

  Важно! Поддерживаются редакции:

  - Windows 7 Профессиональная
  - Windows 7 Корпоративная
  - Windows 7 Максимальная

  По причине отсутствия поддержки удаленного запуска программ не поддерживаются следующие редакции:

  - Windows 7 Начальная
  - Windows 7 Домашняя базовая
  - Windows 7 Домашняя расширенная

- **Windows Server 2008 R2**

  Для системы Windows 2008 должен быть установлен пакет обновления 2.

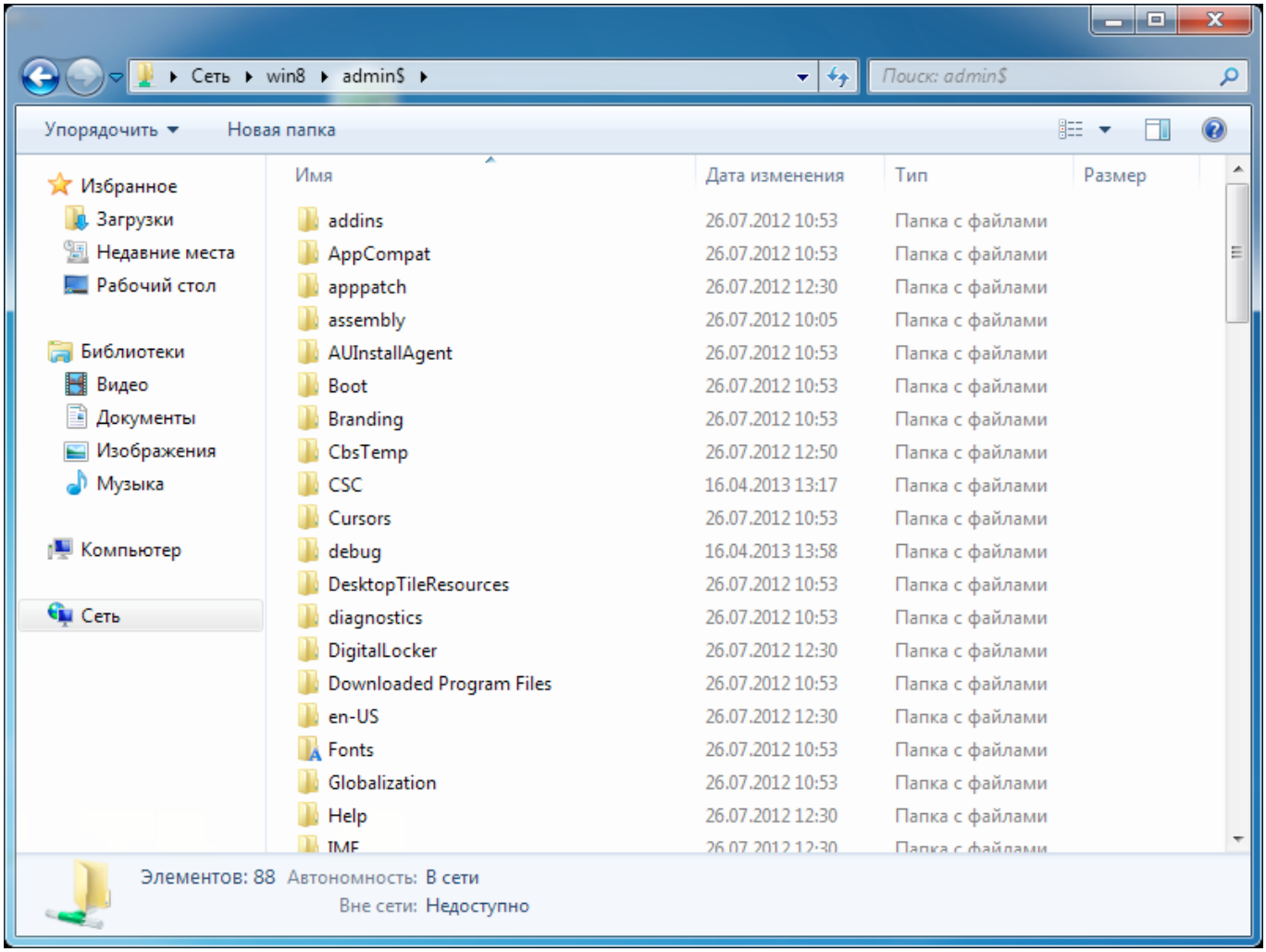
  Загрузить пакет обновления 2 для Windows 2008:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Подключение станций к сети Интернет не требуется.

Убедитесь, что на машине доступны общие административные ресурсы. Для этого перейдите в сетевую папку admin$ на удаленном компьютере. В зависимости от настроек Windows может понадобиться ввод логина и пароля для авторизации под учетной записью администратора. В результате должна открыться сетевая папка (см. рис. ниже).



В случае недоступности общих административных ресурсов выполните на машине следующие настройки.

Откройте редактор реестра (regedit), откройте ветку

[HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANSERVER\PARAMETERS]

Создайте параметр типа DWORD 32 бита «AutoShareWks» (без кавычек), присвойте ему значение, равное единице. Перезагрузите компьютер. Будут включены общие административные ресурсы.

Для антивирусной проверки станций требуется одновременное выполнение следующих условий:

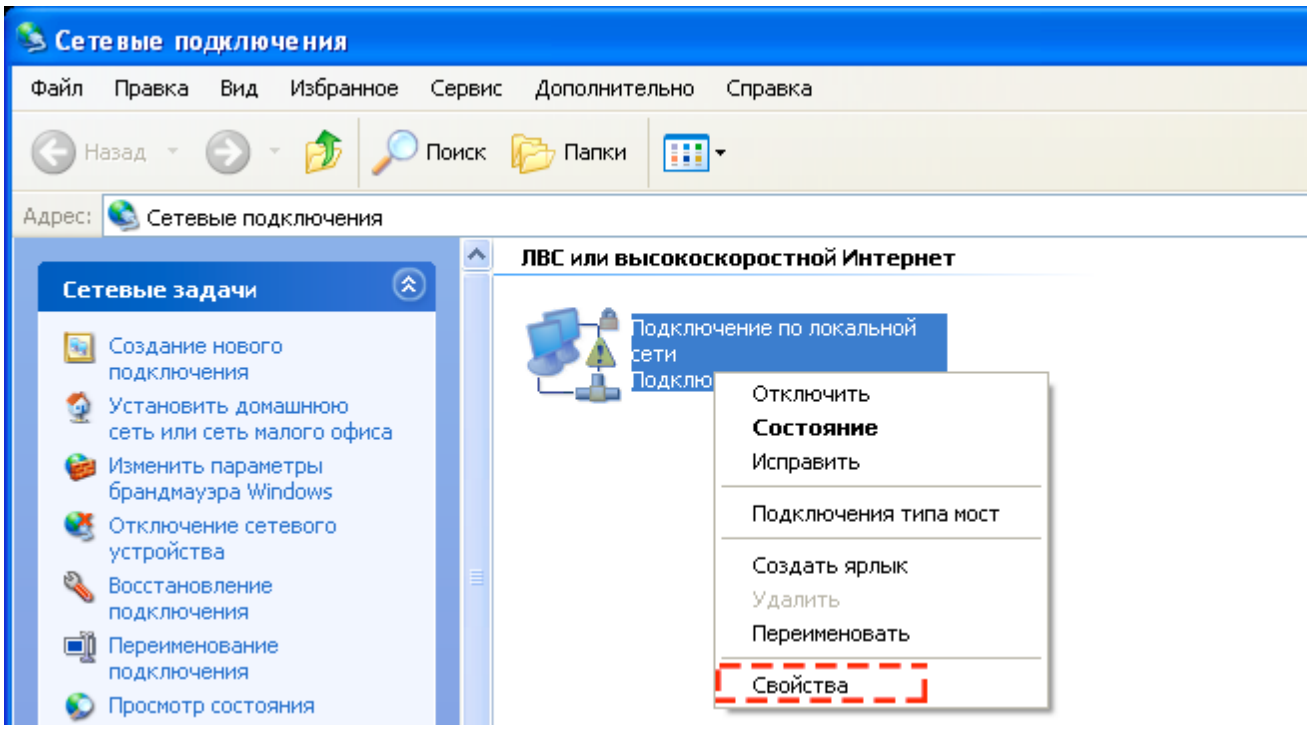
- опция **Сетевое обнаружение** должна быть включена на компьютере, на котором запущен Мастер, если вы планируете искать станции в сети этим методом;
- станция должна быть доступна по сети;
- используемая для подключения учетная запись должна существовать и обладать необходимыми правами;
- если для защиты удаленного компьютера используется брандмауэр, необходимо провести дополнительные настройки, описанные ниже;

- ограничения системы контроля учетных записей (UAC) должны быть отключены, если станция работает под управлением Windows Vista или более поздней операционной системы. Если вы работаете под встроенным аккаунтом администратора, то данную настройку проводить не нужно;
- все необходимые для работы сети службы должны быть установлены и настроены.

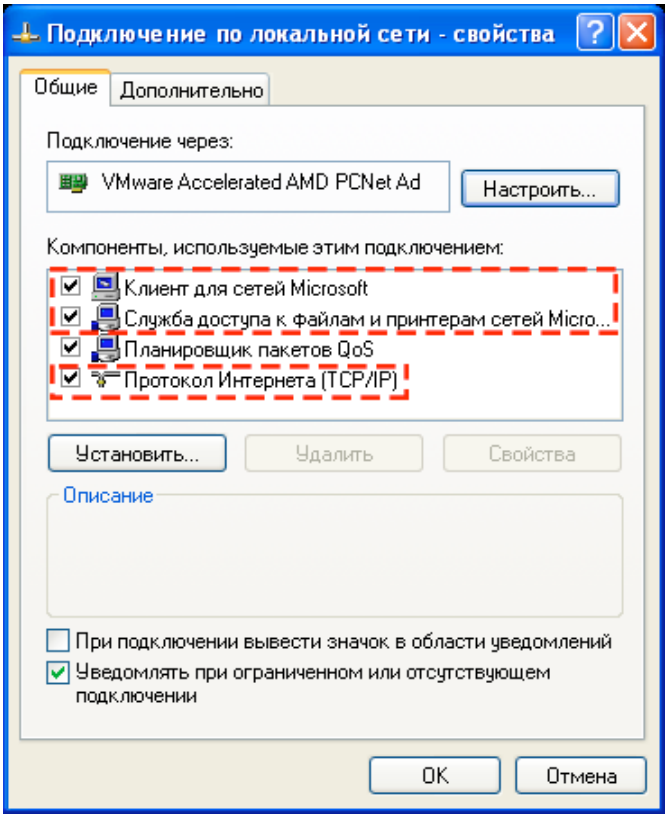
Проверка сетевых настроек

1. Запустите **Панель управления** на станции любым из способов:

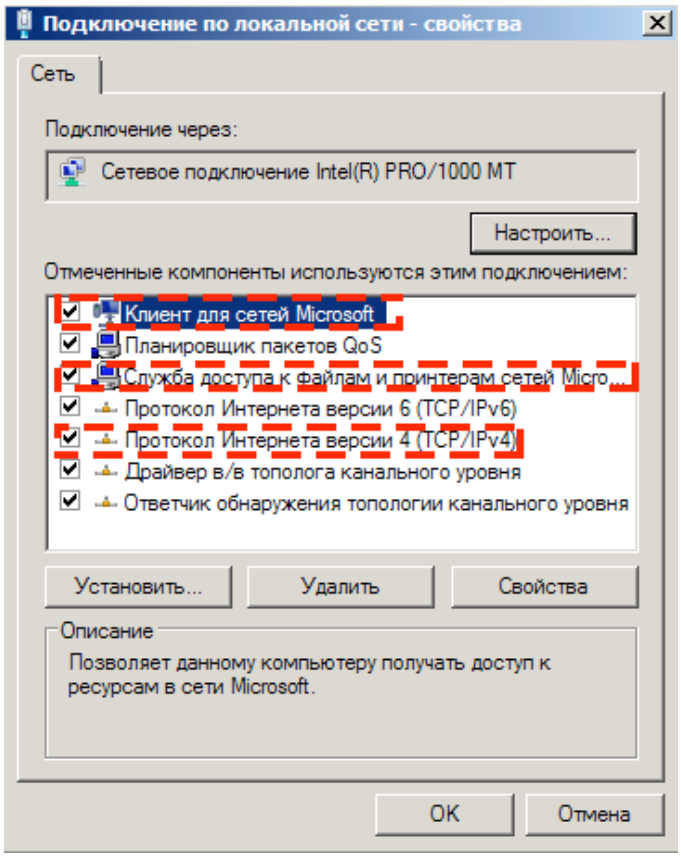
- для систем Windows XP/2003Vista нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Сетевые подключения** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**). Наведите курсор мыши на сетевое подключение и нажмите левую клавишу мыши. Откроется контекстное меню, выберите в нем пункт **Свойства**.



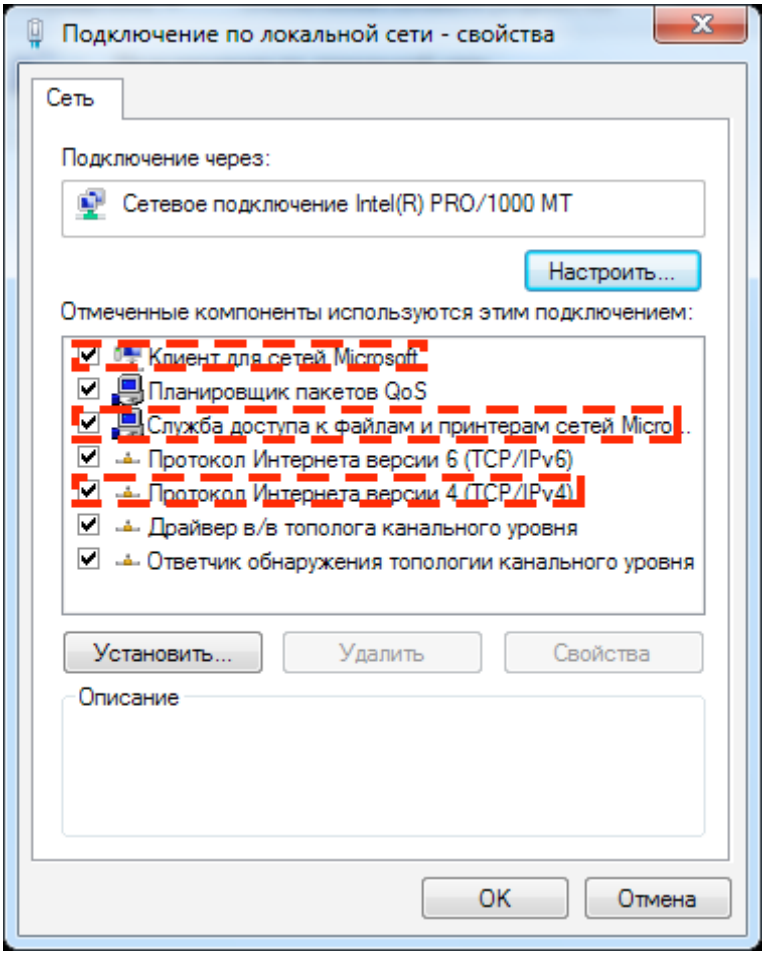
Перейдите на вкладку **Общие**.



- для Windows Vista нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Управление сетевыми подключениями**. Наведите курсор мыши на сетевое подключение и нажмите левую клавишу мыши. Откроется контекстное меню, выберите в нем пункт **Свойства**.



- для Windows 7 или Windows Server 2008 нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера**. С помощью курсора выделите сетевое подключение и нажмите правую клавишу мыши. Откроется контекстное меню, выберите в нем пункт **Свойства**. Убедитесь, что включены следующие компоненты:



  - для Windows 8, Windows 10 или Windows Server 2012 нажмите на кнопки **Windows + X**. В открывшемся контекстном меню выберите пункт **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера**. С помощью курсора выделите сетевое подключение и нажмите правую клавишу мыши. Откроется контекстное меню, выберите в нем пункт **Свойства**;
  - для Windows 10 в категории **Сеть и Интернет** перейдите в любую из вкладок **VPN**, **Ethernet** или **Набор номера**, выберите **Центр управления сетями и общим доступом → Изменение параметров адаптера**.

2. Проверьте, что для выбранного подключения установлены и настроены следующие службы:
   - клиент для сетей Microsoft;
   - служба доступа к файлам и принтерам сетей Microsoft;
   - протокол Интернета версии 4 (TCP/IPv4) или версии 6 (TCP/IPv6).
3. Сохраните изменения и закройте окно настроек.

- Параметры общего доступа должны допускать расширенную настройку, описанную ниже.
- Для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности, настройка которой описана ниже.

- Если в организации используется контроллер домена Active Directory, следует настроить параметры общего доступа к файлам и принтерам, параметры безопасности. Вы можете создать новый объект групповой политики (GPO) для применения данных настроек или же изменить параметры уже существующего объекта.

Создание нового объекта групповой политики

1. В окне командной строки введите в текстовое поле **gpmc.msc** и запустите консоль управления групповыми политиками **GPMC**.
2. Создайте новый объект групповой политики, например **GPO-CureNet**. Для этого в дереве консоли **GPMC** правой кнопкой мыши щелкните **Объекты групповой политики** в соответствующем лесу и домене. Нажмите **Создать**. В открывшемся диалоговом окне укажите имя нового объекта и нажмите **OK**.
3. Привяжите созданный объект к нужному домену.
4. Правой кнопкой мыши нажмите на созданный объект, выберите **Изменить** и скорректируйте необходимые настройки в соответствие с описанием, приведенным ниже.

Если вы решили не создавать новый объект, а изменить параметры уже существующего объекта, то откройте окно с соответствующими настройками.

1. На компьютере, где установлена консоль управления групповыми политиками GPMC, нажмите **Пуск → Администрирование → Управление групповой политикой**.
2. Если появится диалоговое окно контроля учетных записей, поверьте данные и нажмите кнопку **Продолжить**.
3. В области навигации найдите и разверните узел **Лес: Имя леса**, затем разверните узел **Объекты групповой политики** и щелкните правой кнопкой мыши имя того объекта, для которого вы хотите задать разрешение.
4. В открывшемся меню выберите **Изменить**.

Настройка общего доступа к файлам и принтерам

Разрешите входящие запросы на доступ к файлам от клиентских компьютеров. Включение данного исключения брандмауэра открывает для IP-адресов, указанных в данном правиле, UDP-порты 137 и 138, а также TCP-порт 445.

Разрешение общего доступа к файлам и принтерам

1. В области навигации открывшегося окна разверните следующие узлы: **Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Сетевые подключения → Брандмауэр Windows → Профиль домена**.
2. В области сведений дважды щелкните по настройке **Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам** и включите данное правило на вкладке настроек.
3. В текстовом поле **Разрешить незапрошенные входящие сообщения с этих IP-адресов** укажите нужный диапазон.
4. Нажмите **ОК**, чтобы сохранить изменения.

Настройка параметров безопасности

Настройте политику **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** так, чтобы при входе в сеть с учетными данными локальной учетной записи проверка подлинности производилась по этим данным.

Разрешение сетевого доступа по учетным записям пользователей

1. В области навигации открывшегося окна разверните следующие пункты: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности →Локальные политики → Параметры безопасности**.
2. Для политики **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** установите режим **Обычная — локальные пользователи удостоверяются как они сами**.

Применение изменений в домене

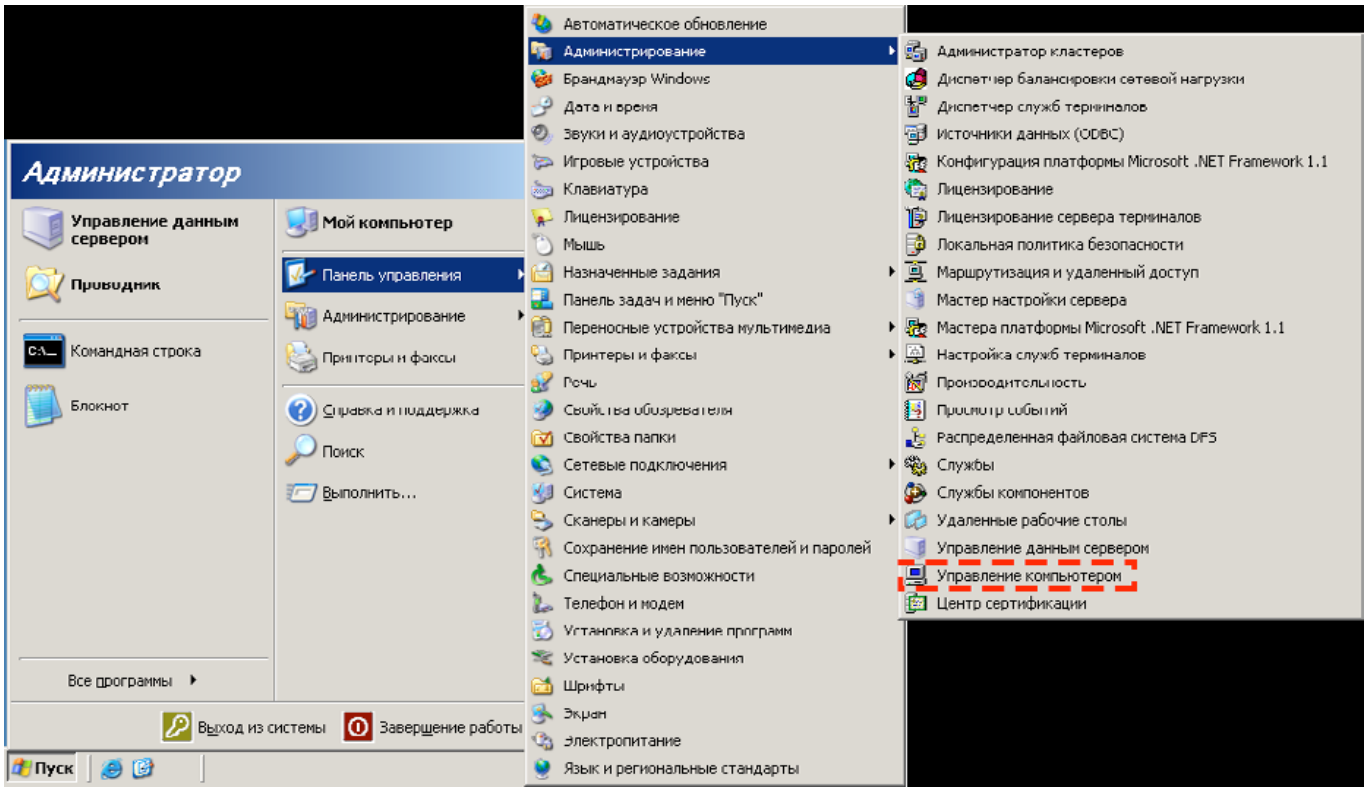
Для того чтобы применить изменения групповых политик в домене, в обоих случаях (и при создании нового объекта, и при изменении политик уже существующего объекта) в окне командной строки укажите команду **gpupdate /force**.

Создание учетной записи для подключения

Используемая для подключения учетная запись должна существовать и обладать необходимыми правами.

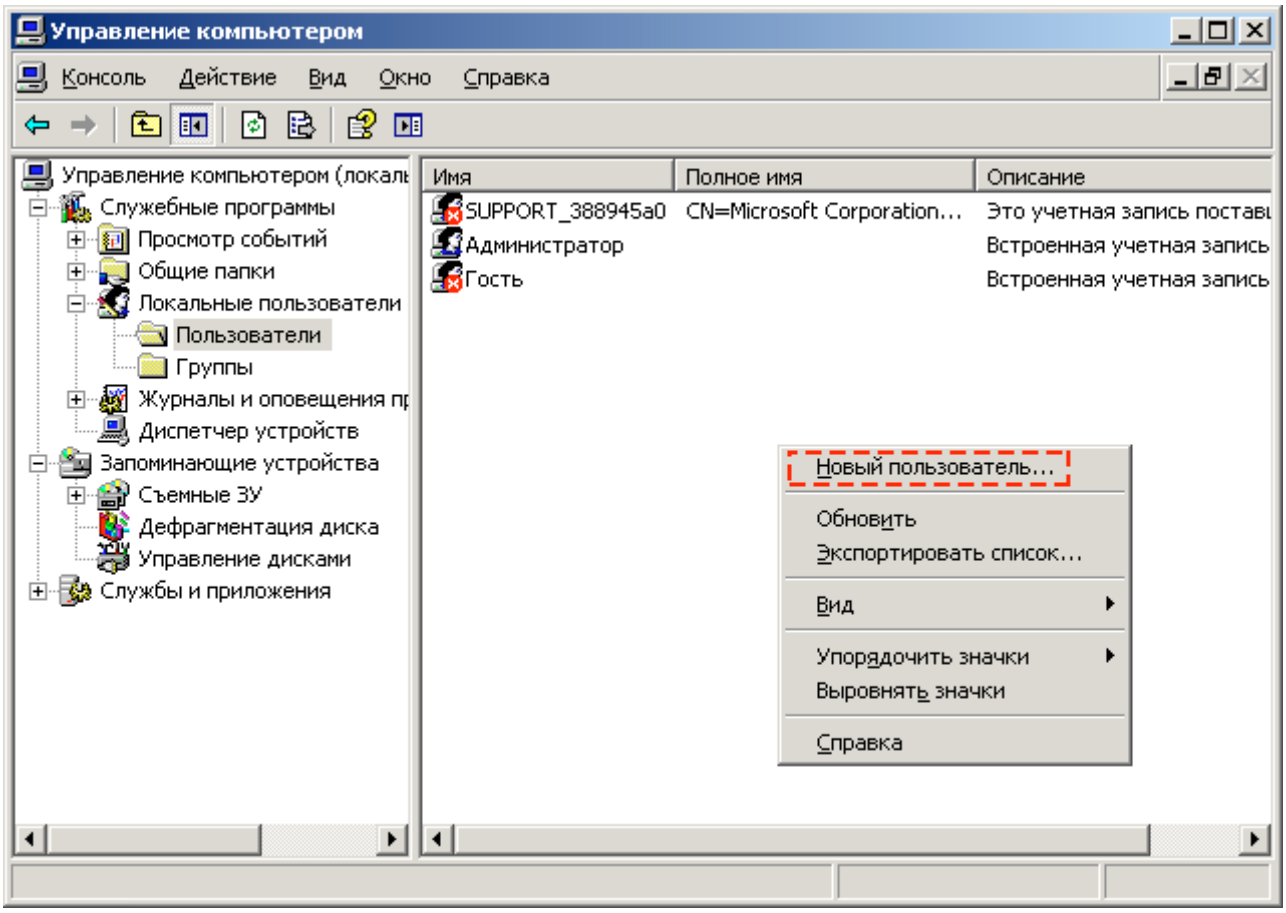
- **Windows XP, Windows 2003**

  Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи**.

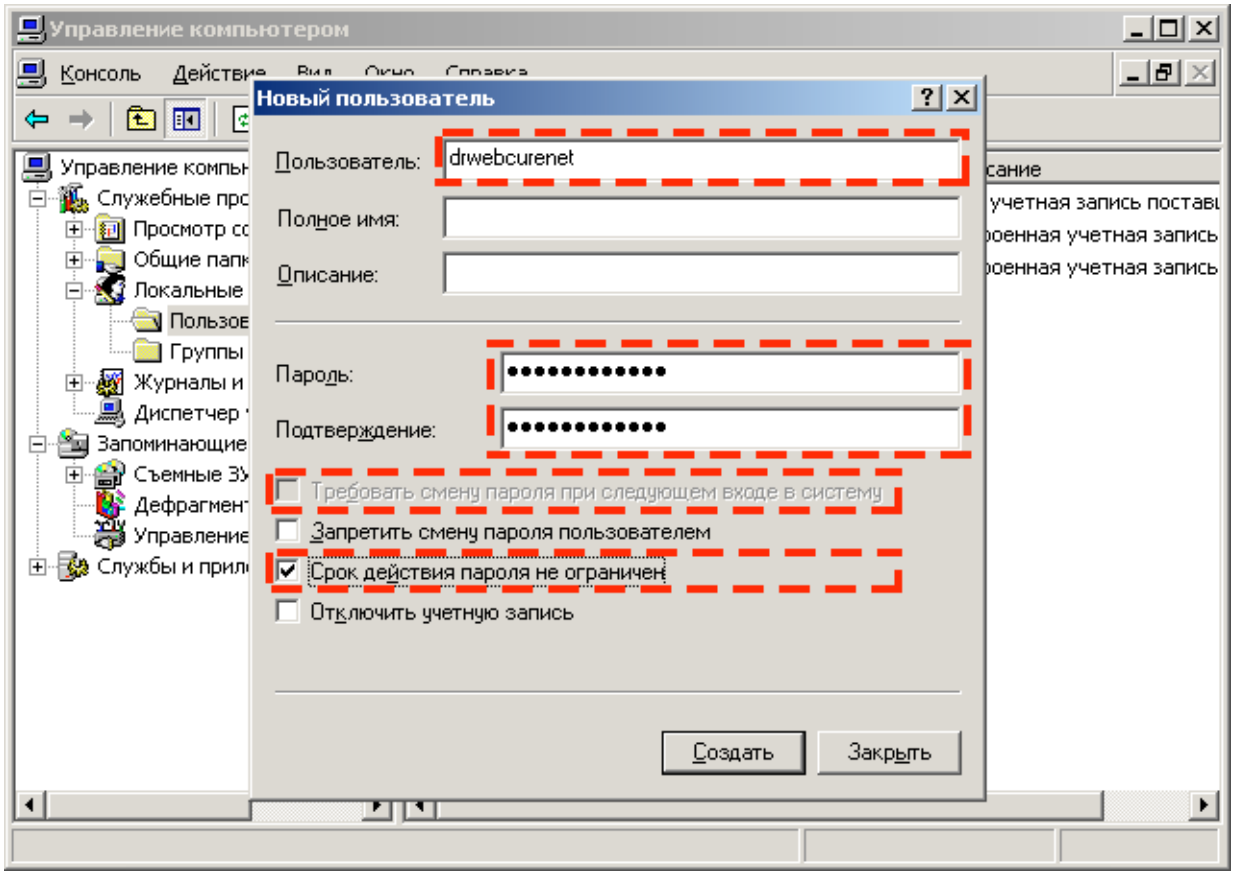


Дальнейшие манипуляции можно выполнять со стандартной учетной записью **Администратор**, но в целях увеличения секретности рекомендуется создать альтернативную

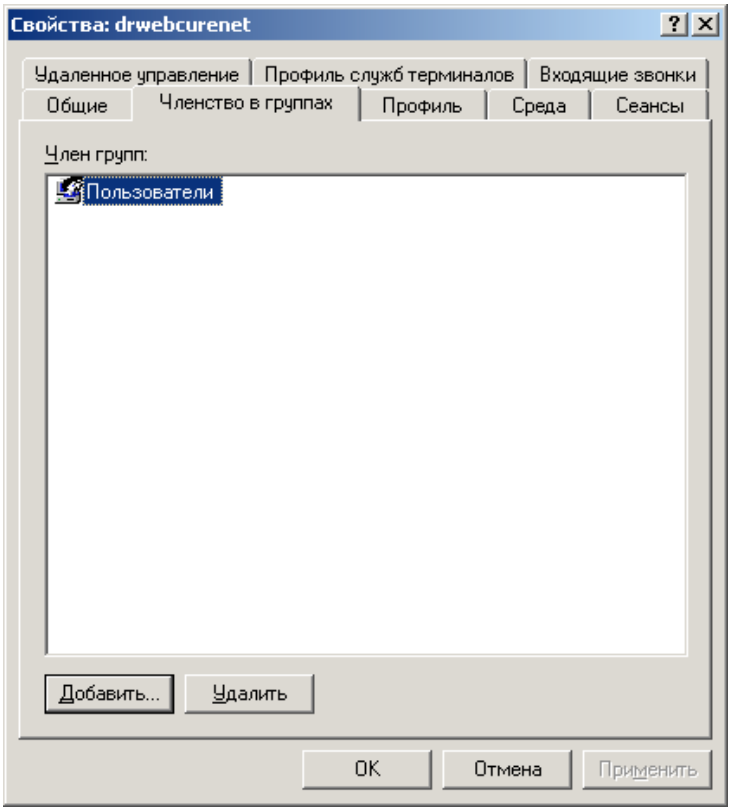
учетную запись администратора. Для этого в правой части окна щелкните правой клавишей мыши. В появившемся контекстном меню выберите пункт **Новый пользователь**.



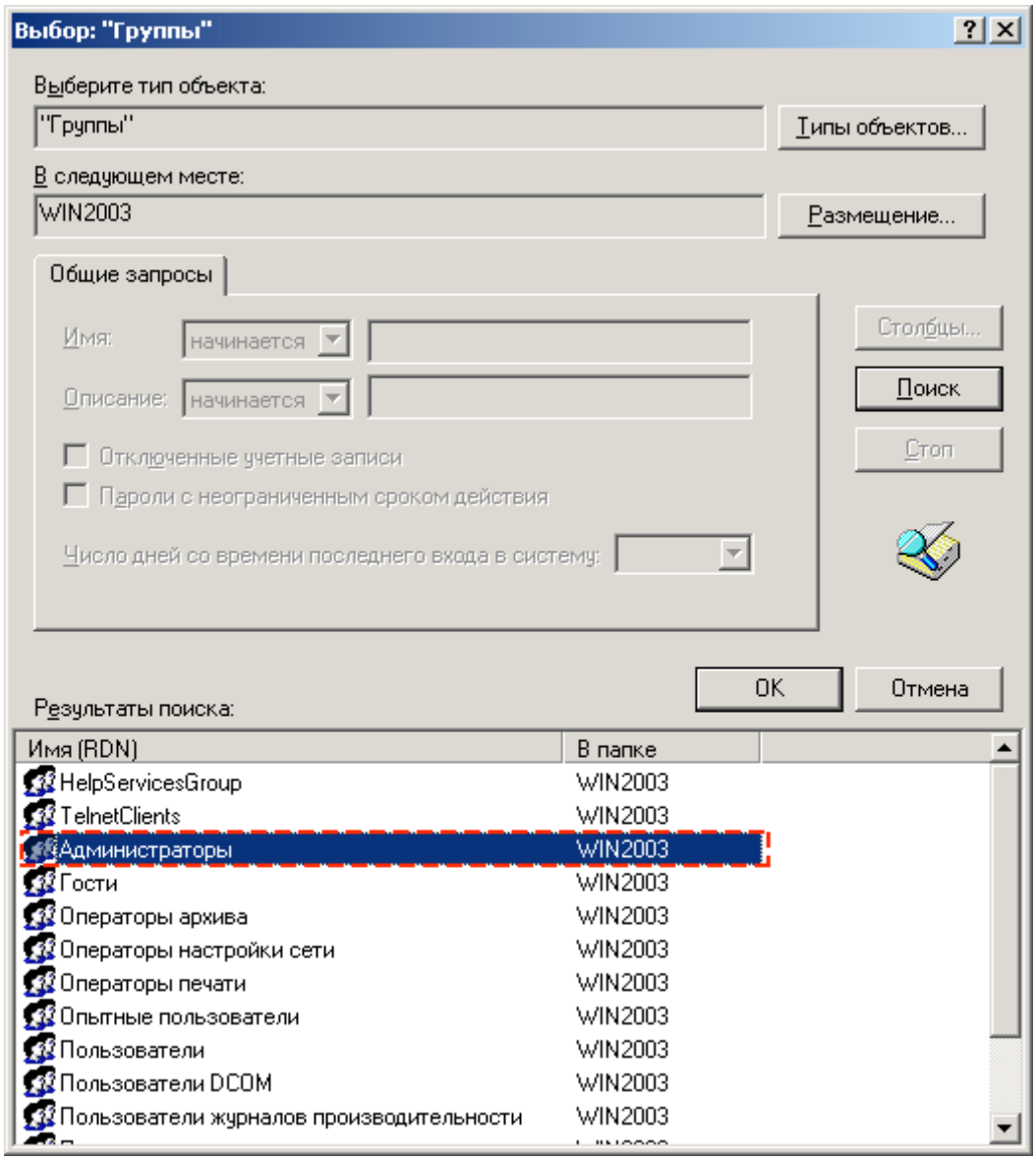
Введите имя пользователя **DrWebCurenet**, в полях **Пароль** и **Подтверждение** введите сложный пароль. Отключите опцию **Потребовать смену пароля при следующем входе в систему**. Включите опцию **Срок действия пароля не ограничен**. Нажмите на кнопку **Создать**, затем нажмите на кнопку **Закрыть**.

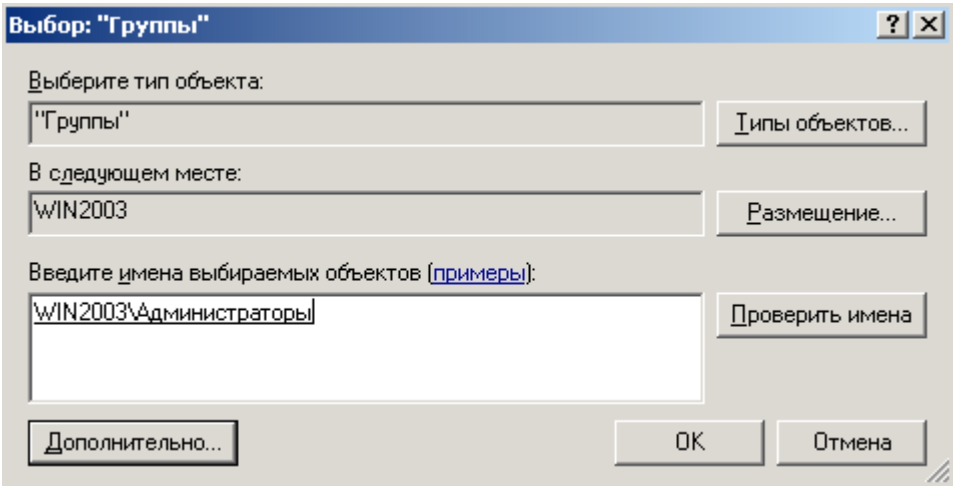


Дважды щелкните по созданной записи **DrWebCurenet**. Откроется окно **Свойства DrWebCurenet**. Перейдите на вкладку **Членство в группах**.



В окне **Член групп:** выделите **Пользователи** и нажмите на кнопку **Удалить**. Затем нажмите на кнопку **Добавить**. Откроется окно **Выбор: Группы**. Нажмите на кнопку **Дополнительно**, затем нажмите на кнопку **Поиск**. В сформировавшемся списке выберите **Администраторы**, нажмите на кнопку **ОК**, а затем — нажмите на кнопку **ОК** в окне **Выбор: Группы**.

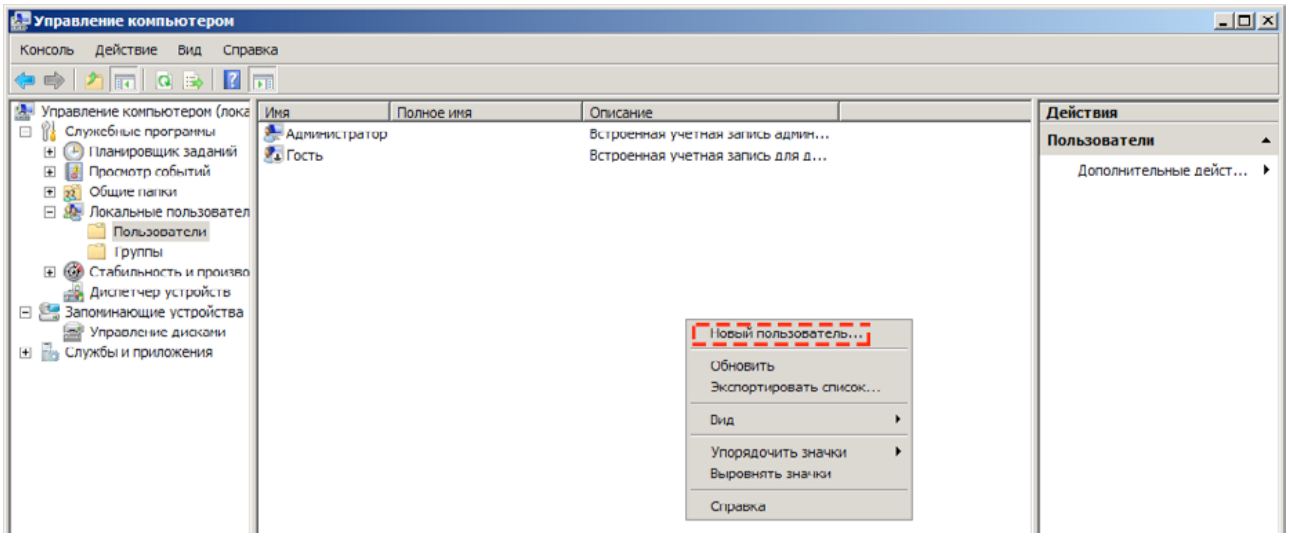




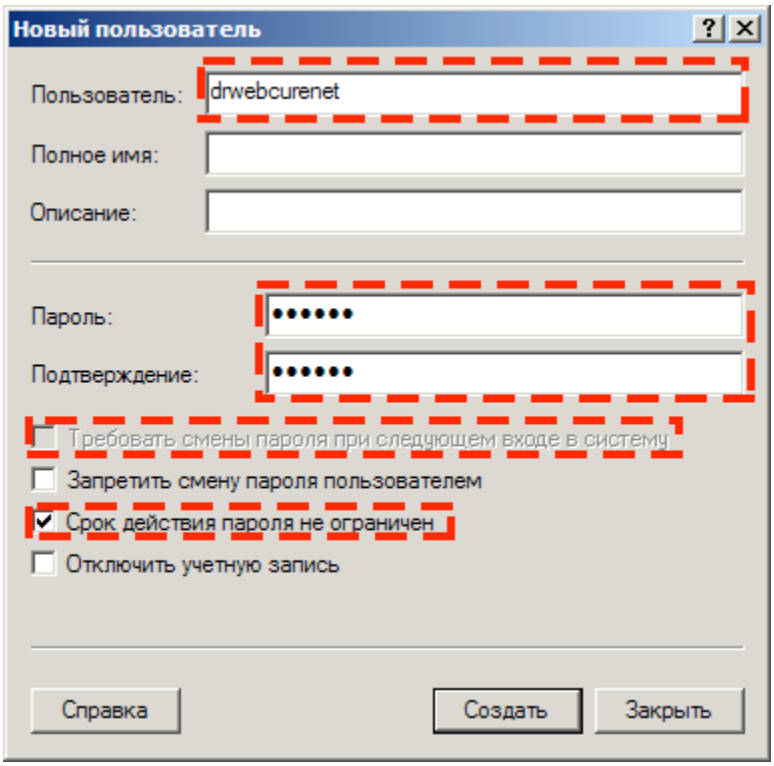
В окне **Свойства: Dr.WebCureNet** нажмите последовательно на кнопки **Применить** и **ОК**.

- **Windows Vista и Windows Server 2008**

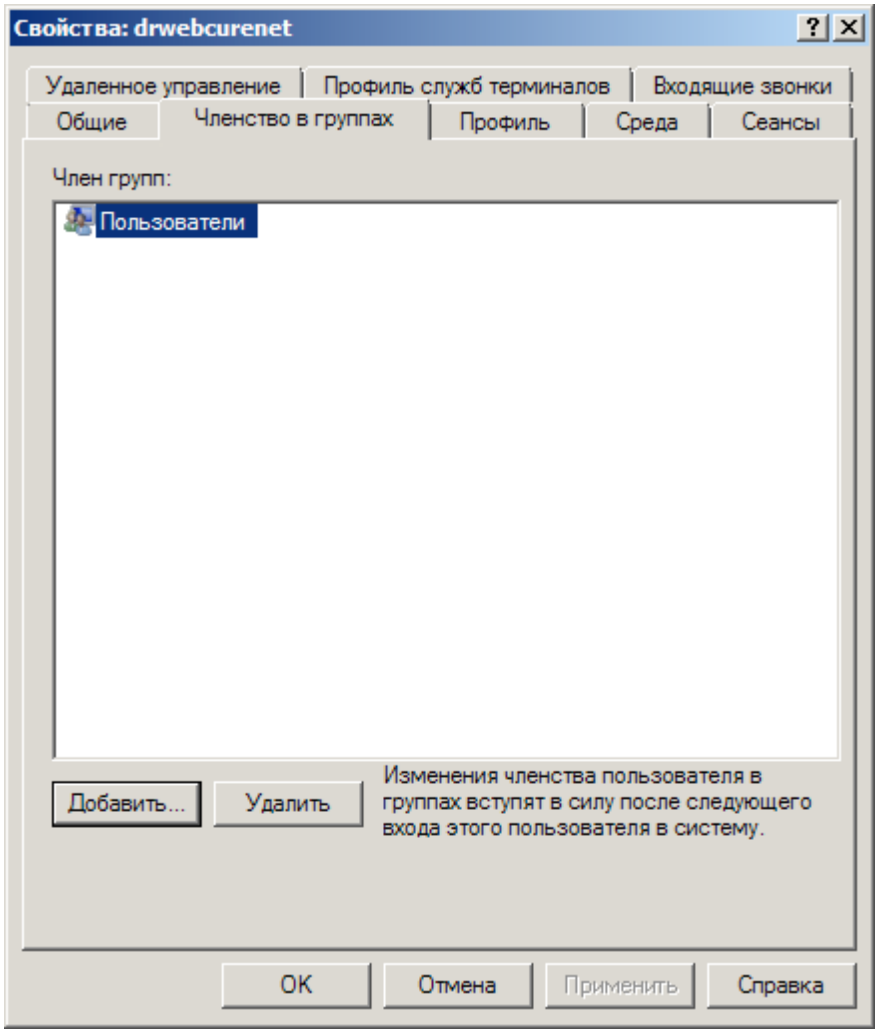
  Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Система и ее обслуживание → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи**. Дальнейшие манипуляции можно выполнять со стандартной учетной записью Администратор, но в целях увеличения секретности рекомендуется создать альтернативную учетную запись администратора. В среднем окне нажмите правую клавишу мыши и в контекстном меню выберите пункт Новый пользователь.



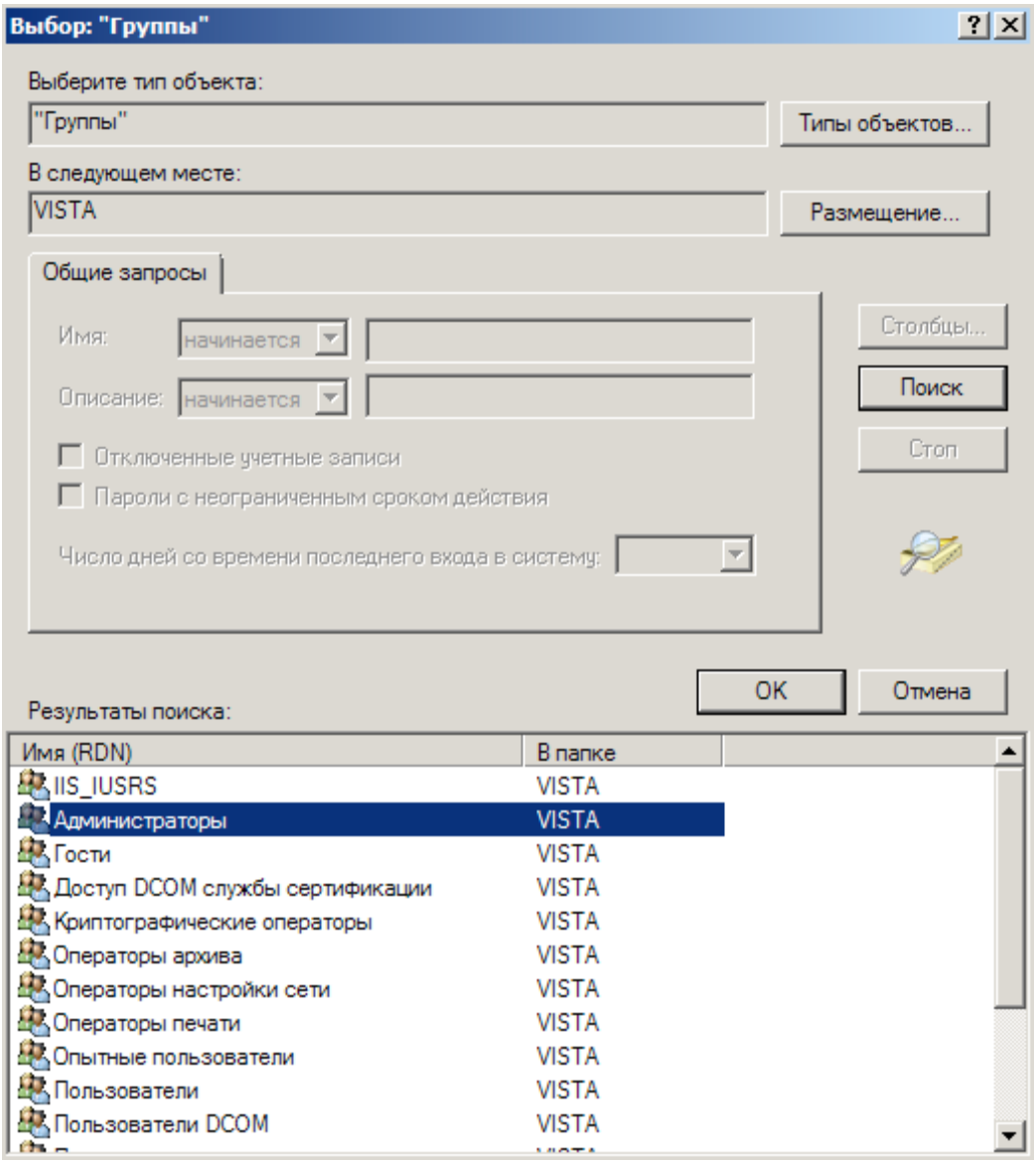
Введите имя пользователя — **DrWebCurenet**. В полях **Пароль** и **Подтверждение пароля** задайте сложный пароль. Снимите флаг **Требовать смены пароля при следующем входе в систему**. Поставьте флаг **Срок действия пароля не ограничен**.



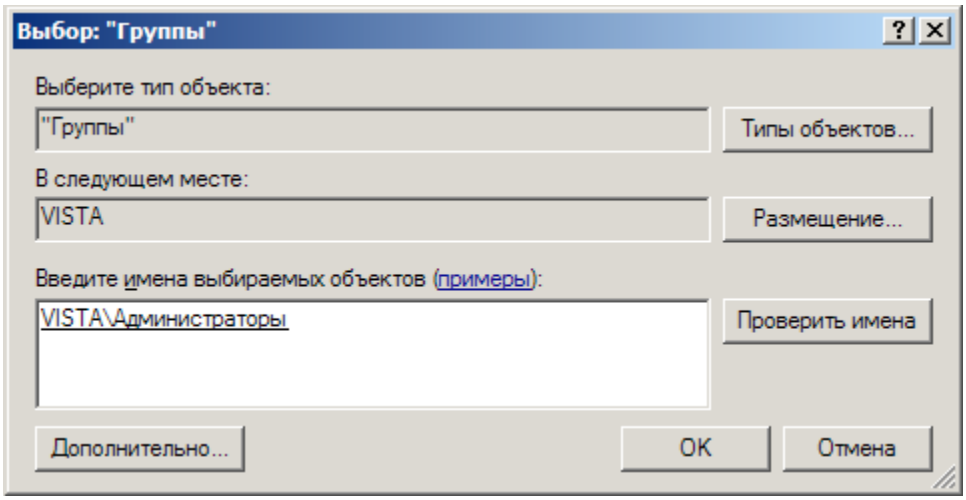
Нажмите последовательно на кнопки **Создать** и **Закрыть**. Левой клавишей мыши дважды щелкните по созданной учетной записи **DrWebCurenet** и перейдите на вкладку **Членство в группах**.


Свойства: drwebcurenet
Удаленное управление
Профиль служб терминалов
Входящие звонки
Общие
Членство в группах
Профиль
Среда
Сеансы
Член групп:
Пользователи
Добавить...
Удалить
Изменения членства пользователя в группах вступят в силу после следующего входа этого пользователя в систему.
OK
Отмена
Применить
Справка

Выделите пункт **Пользователи** и нажмите на кнопку **Удалить**. Затем нажмите на кнопку **Добавить**. Откроется окно **Выбор: Группы**. Нажмите на кнопку **Дополнительно**, затем нажмите на кнопку **Поиск**. В результатах поиска выберите пункт **Администраторы** и нажмите на кнопку **ОК**.



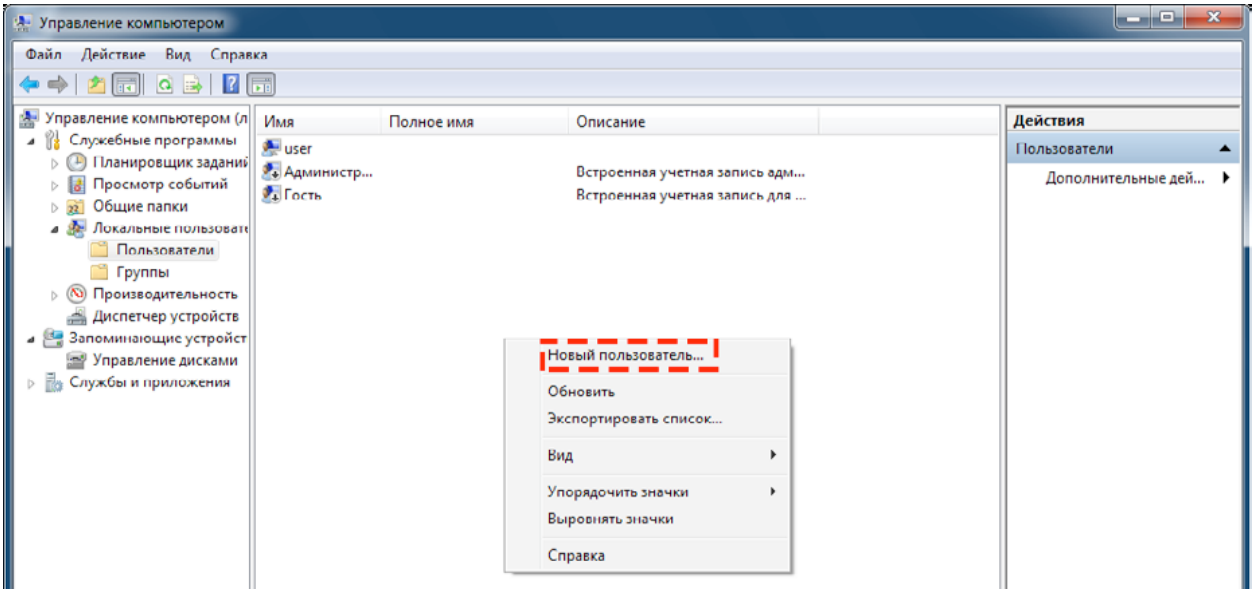
В окне **Выбор: Группы** также нажмите на кнопку **ОК**.



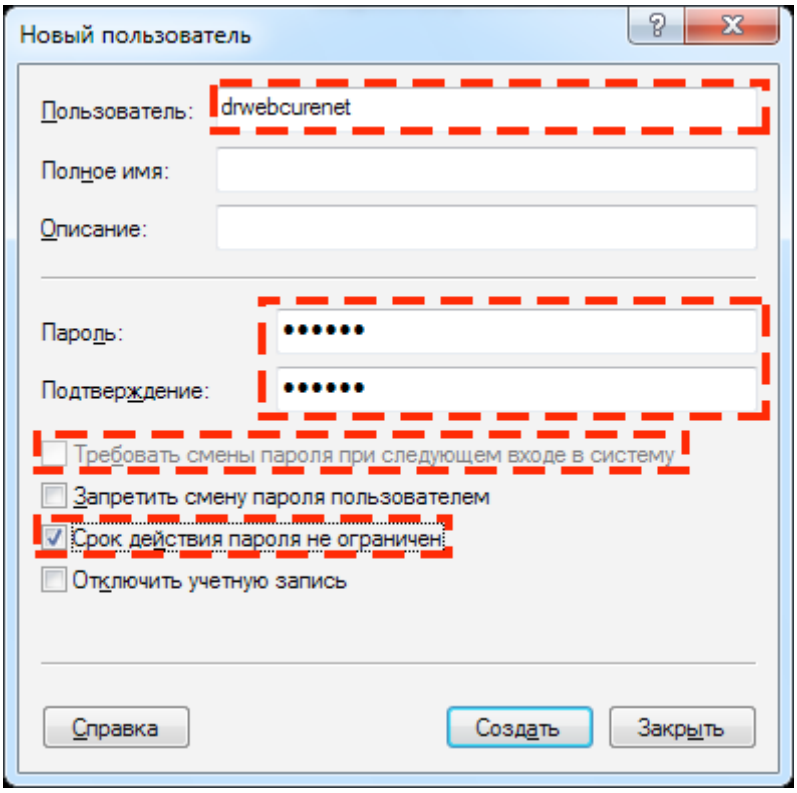
Нажмите последовательно на кнопки **Применить** и **ОК** в окне **Свойства: DrWebCurenet**.

- **Windows 7, Windows 2008 R2**

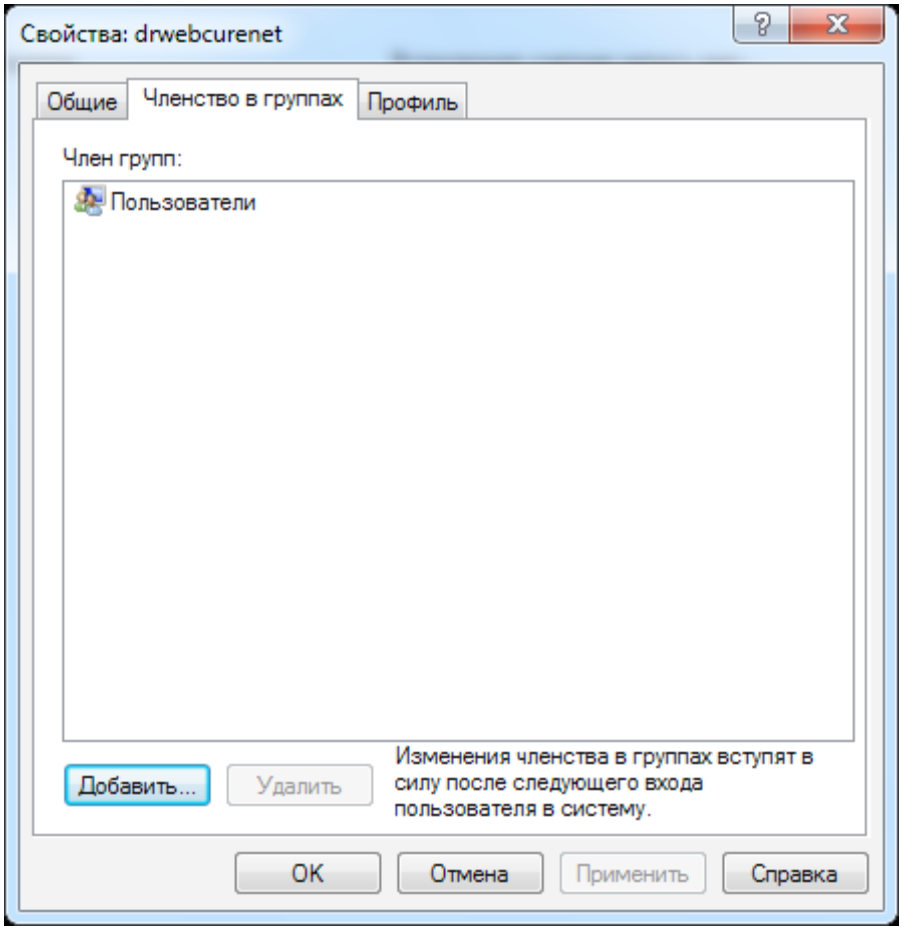
Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Система и безопасность → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи**. Дальнейшие манипуляции можно выполнить со стандартной учетной записью **Администратор**, но в целях увеличения секретности рекомендуется создать альтернативную учетную запись администратора. В среднем окне нажмите правую клавишу мыши и в контекстном меню выберите пункт **Новый пользователь**.



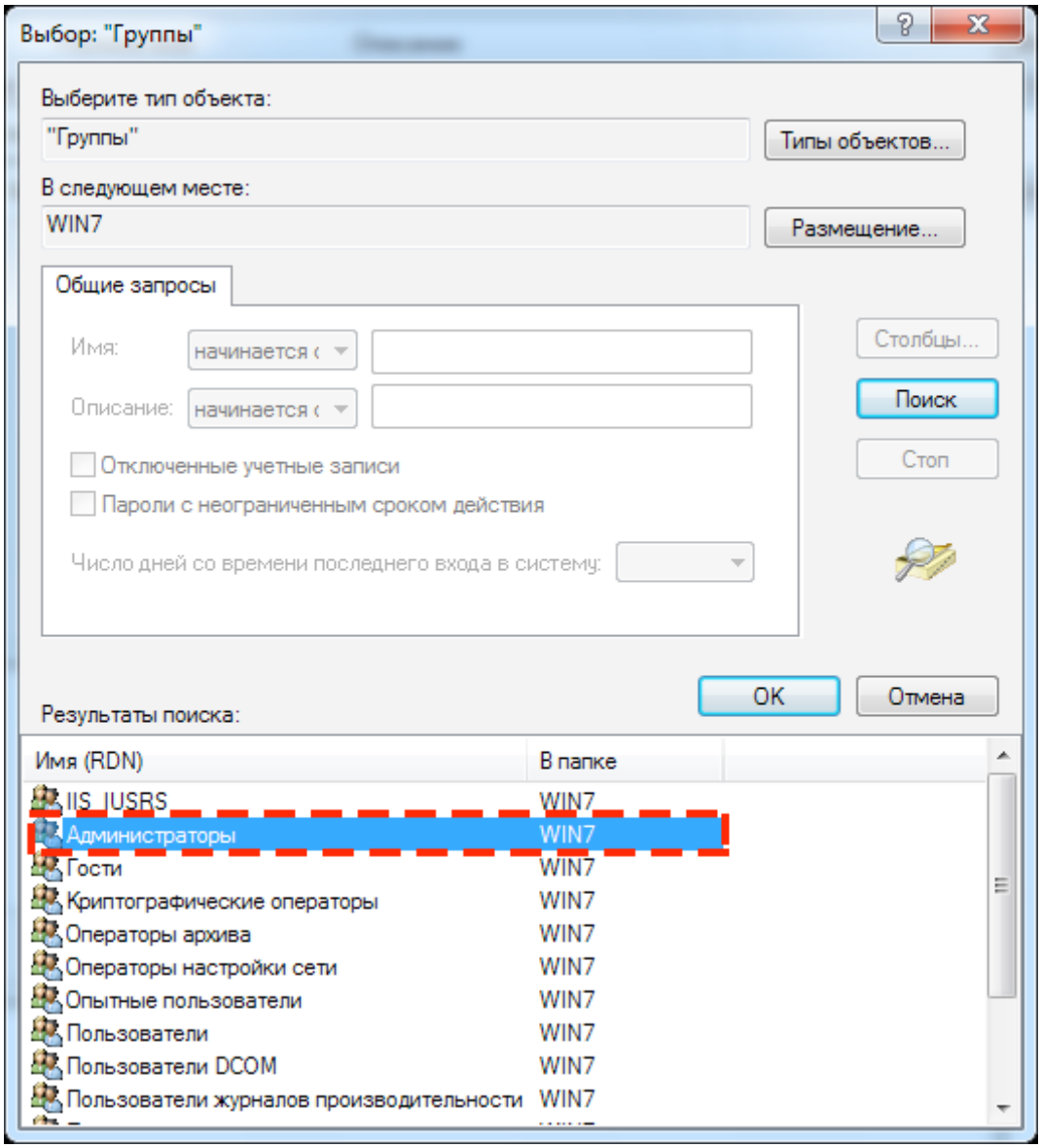
Введите имя пользователя — **DrWebCurenet**. В полях **Пароль** и **Подтверждение пароля** задайте сложный пароль. Снимите флаг **Требовать смены пароля при следующем входе в систему**. Поставьте флаг **Срок действия пароля не ограничен**. Нажмите последовательно на кнопки **Создать** и **Закрыть**.



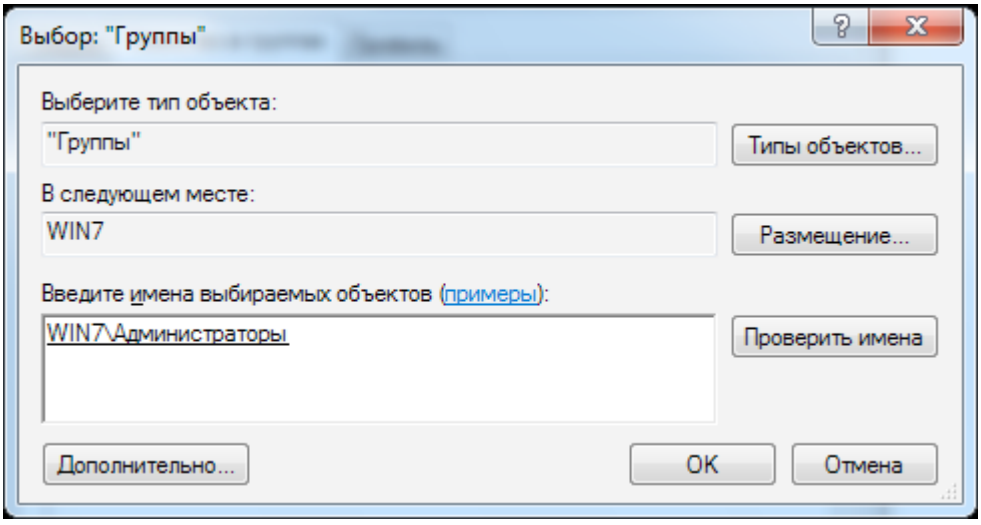
Левой клавишей мыши дважды щелкните по созданной учетной записи **DrWebCurenet** и перейдите на вкладку **Членство в группах**. Выделите пункт **Пользователи** и нажмите на кнопку **Удалить**.



Затем нажмите на кнопку **Добавить**. Откроется окно **Выбор: Группы**. Нажмите на кнопку **Дополнительно**, затем нажмите на кнопку **Поиск**. В результатах поиска выделите курсором мыши пункт **Администраторы** и нажмите на кнопку **ОК**.



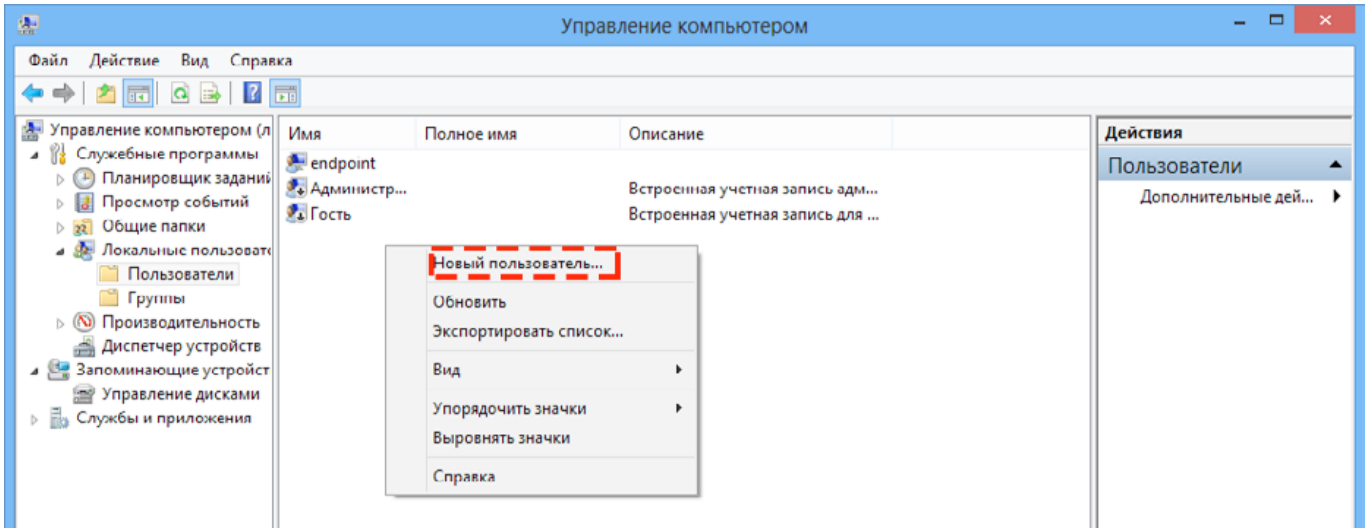
В окне **Выбор: Группы** также нажмите на кнопку **ОК**.



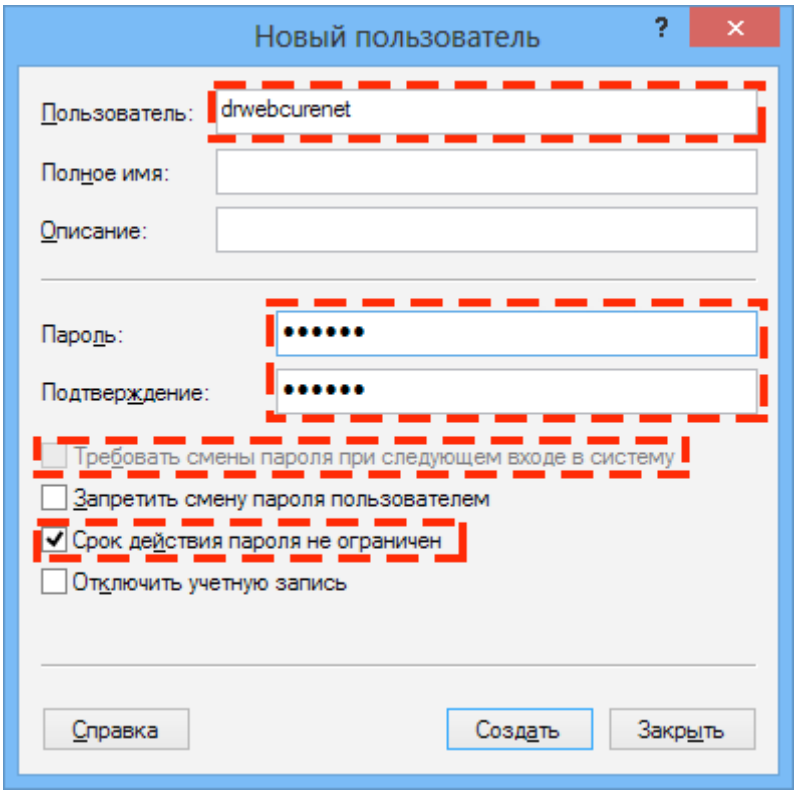
Теперь в окне Свойства: **DrWebCurenet** нажмите последовательно на кнопки **Применить** и **ОК**.

- **Windows 8, 10, Windows 8.1 Windows Server 2012**

Нажмите на кнопки **Windows + X**. В открывшемся контекстном меню выберите пункт **Панель управления → Система и безопасность → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи**. Дальнейшие манипуляции можно выполнить со стандартной учетной записью **Администратор**, но в целях увеличения секретности рекомендуется создать альтернативную учетную запись администратора. В среднем окне нажмите правую клавишу мыши и в контекстном меню выберите пункт **Новый пользователь**.

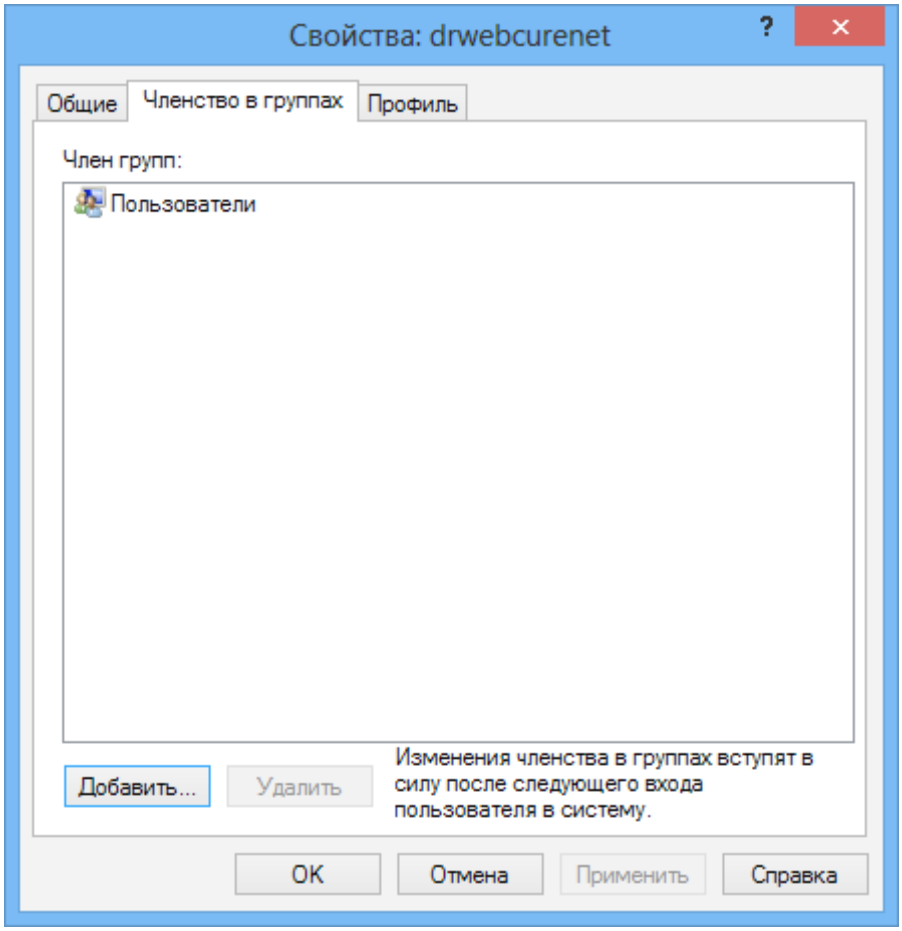


Введите имя пользователя — **DrWebCurenet**. В полях **Пароль** и **Подтверждение пароля** задайте сложный пароль. Снимите флаг **Требовать смены пароля при следующем входе в систему**. Поставьте флаг **Срок действия пароля не ограничен**.



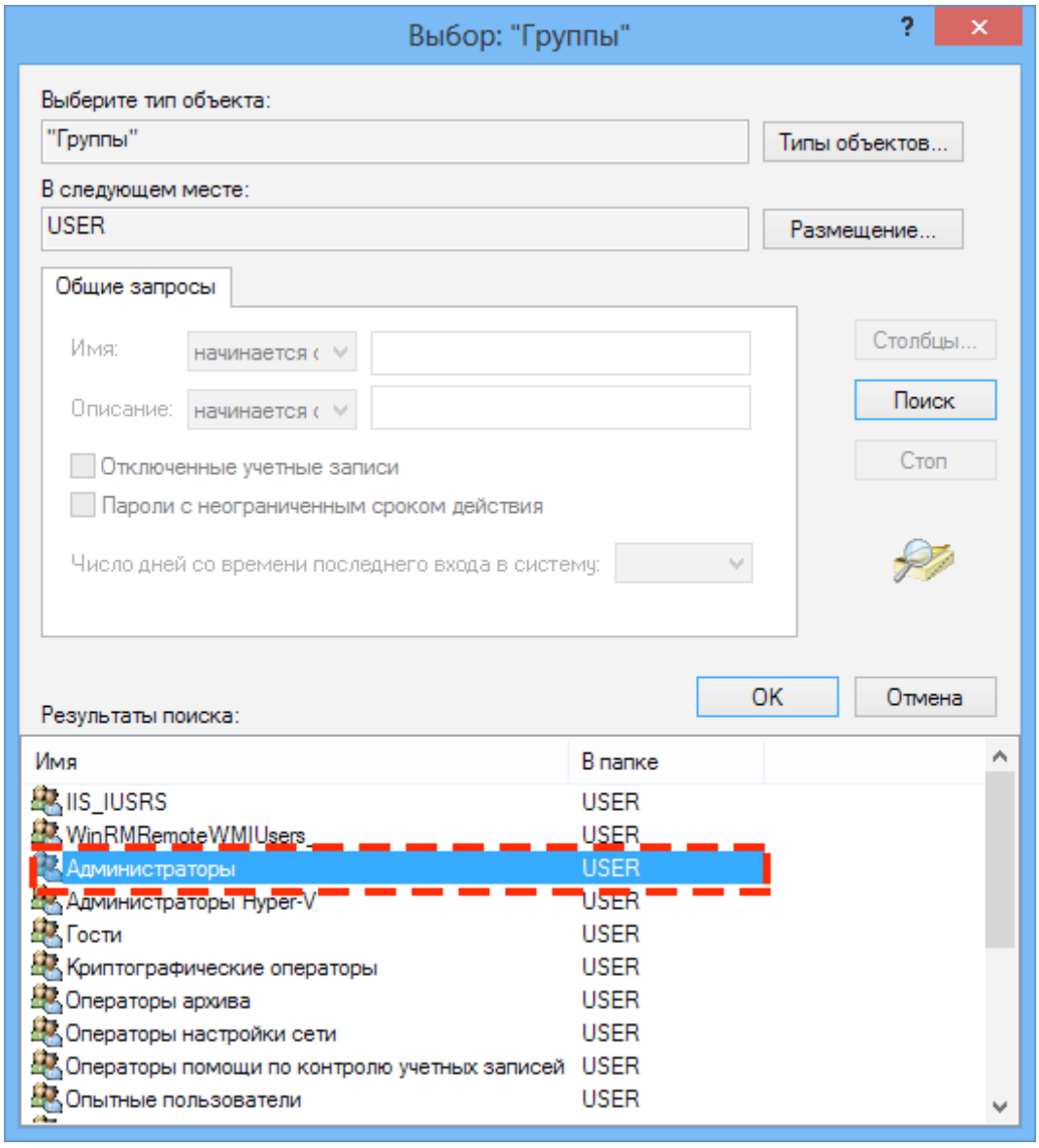
Нажмите последовательно на кнопки **Создать** и **Закрыть**.

Левой клавишей мыши дважды щелкните по созданной учетной записи **DrWebCurenet** и перейдите на вкладку **Членство в группах**.

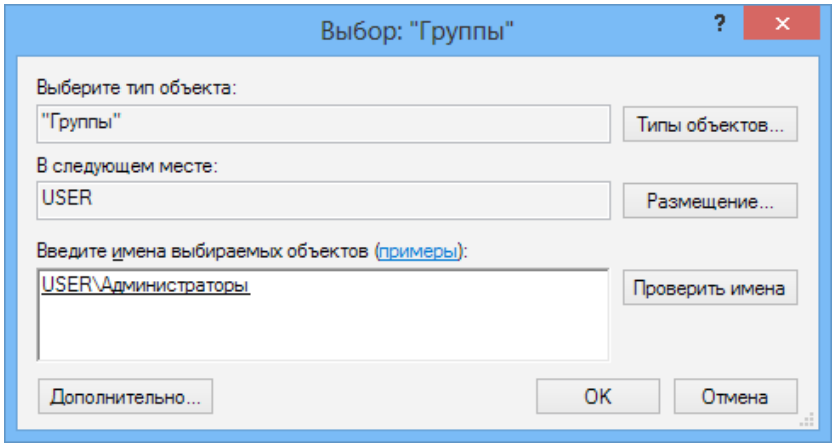


Выделите пункт **Пользователи** и нажмите на кнопку **Удалить**.

Затем нажмите на кнопку **Добавить**. Откроется окно **Выбор: Группы**. Нажмите на кнопку **Дополнительно**, затем нажмите на кнопку **Поиск**. В результатах поиска выделите курсором мыши пункт **Администраторы** и нажмите на кнопку **ОК**.



В окне **Выбор: Группы** также нажмите на кнопку **ОК**.



Теперь в окне **Свойства: DrWebCurenet** нажмите последовательно на кнопки **Применить** и **ОК**.

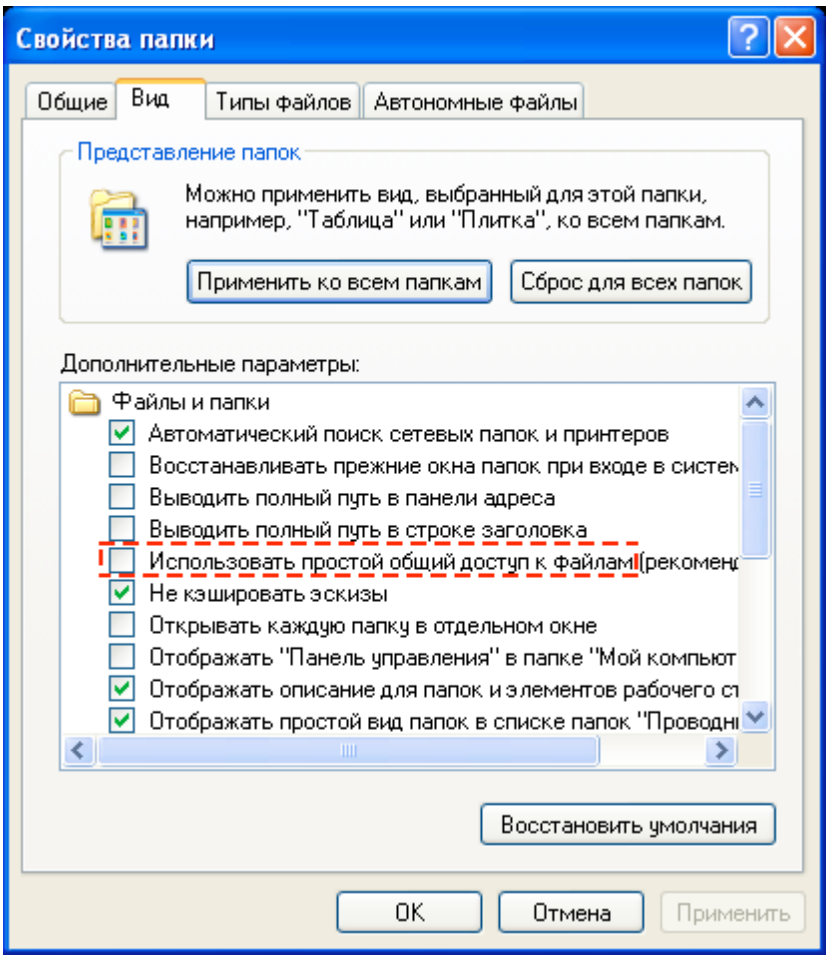
Настройка общего доступа к файлам

- **Windows XP**

Для Windows 2003 данная настройка не требуется.

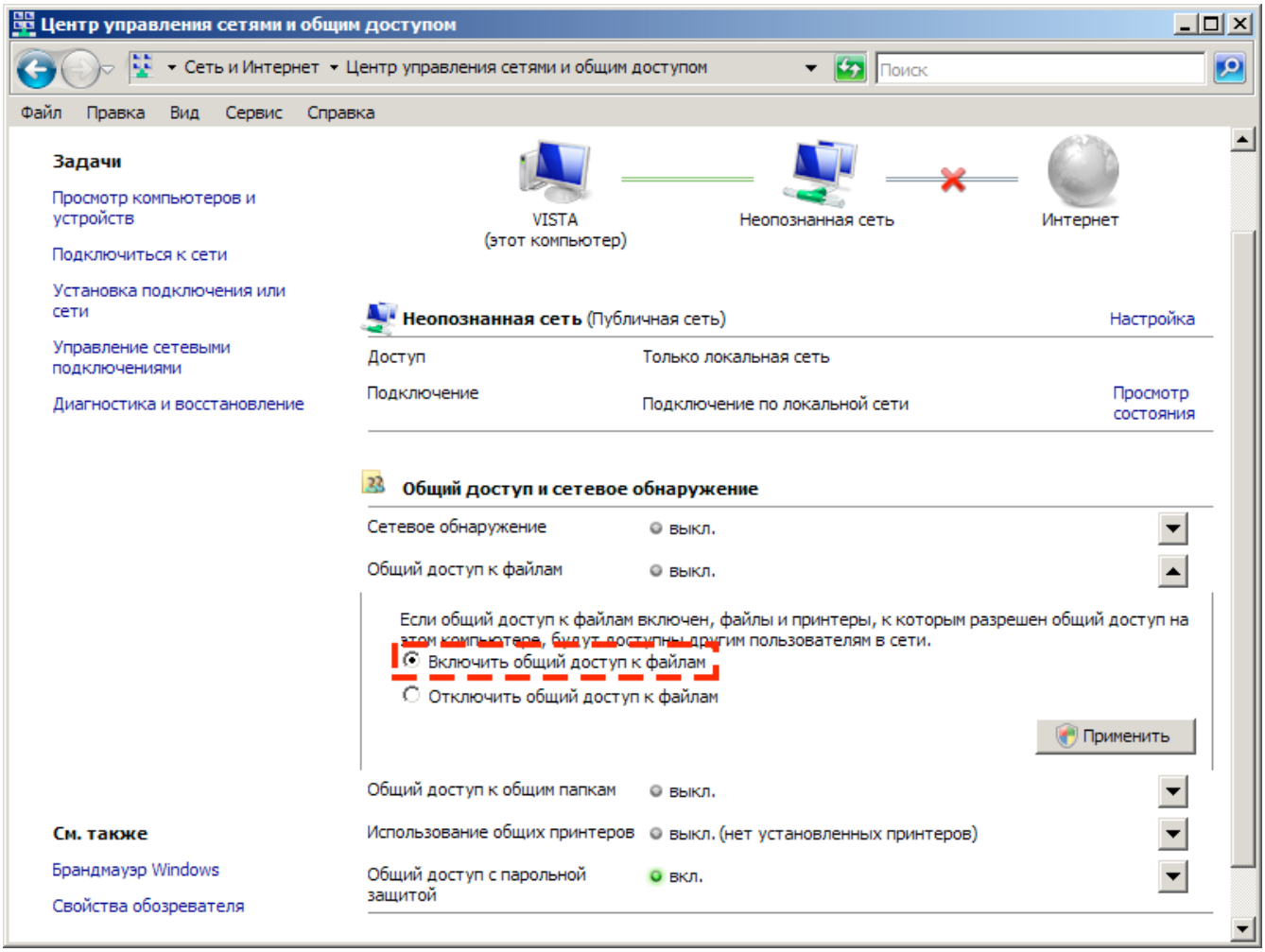
Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Переход к классическому виду → Свойства папки**. Откроется окно **Свойства папки**. Перейдите на вкладку **Вид**. Снимите флаг **Использовать простой общий доступ к файлам**. Нажмите последовательно на кнопки **Применить** и **ОК**.

Вы также можете выполнить эту настройку в Панели управления. Выберите пункт **Брандмауэр Windows** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**). Перейдите на вкладку **Исключения** и включите настройку **Общий доступ к файлам и принтерам**.



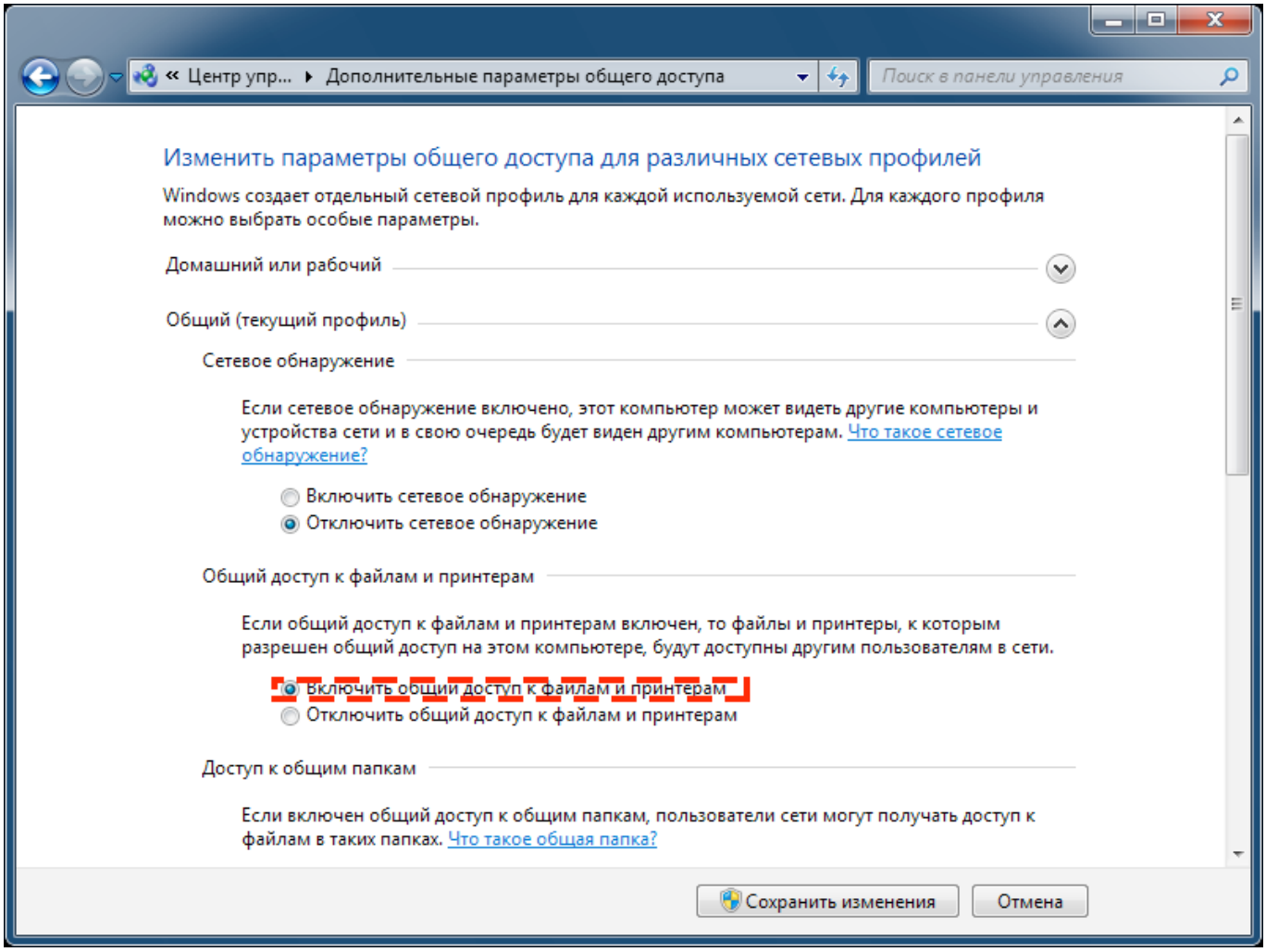
- **Windows Vista, Windows Server 2008**

Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом**. В группе **Общий доступ и сетевое обнаружение** поставьте флаг **Включить общий доступ к файлам**. Нажмите на кнопку **Применить**.



- **Windows 7, Windows Server 2008 R2**

Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа**. В общем сетевом профиле выберите пункты **Включить сетевое обнаружение** и **Включить общий доступ к файлам и принтерам**.

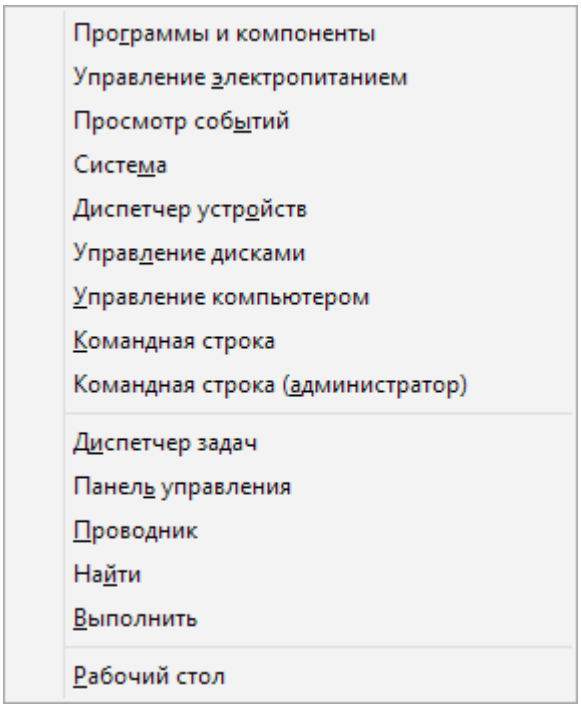


Нажмите на кнопку **Сохранить изменения**.

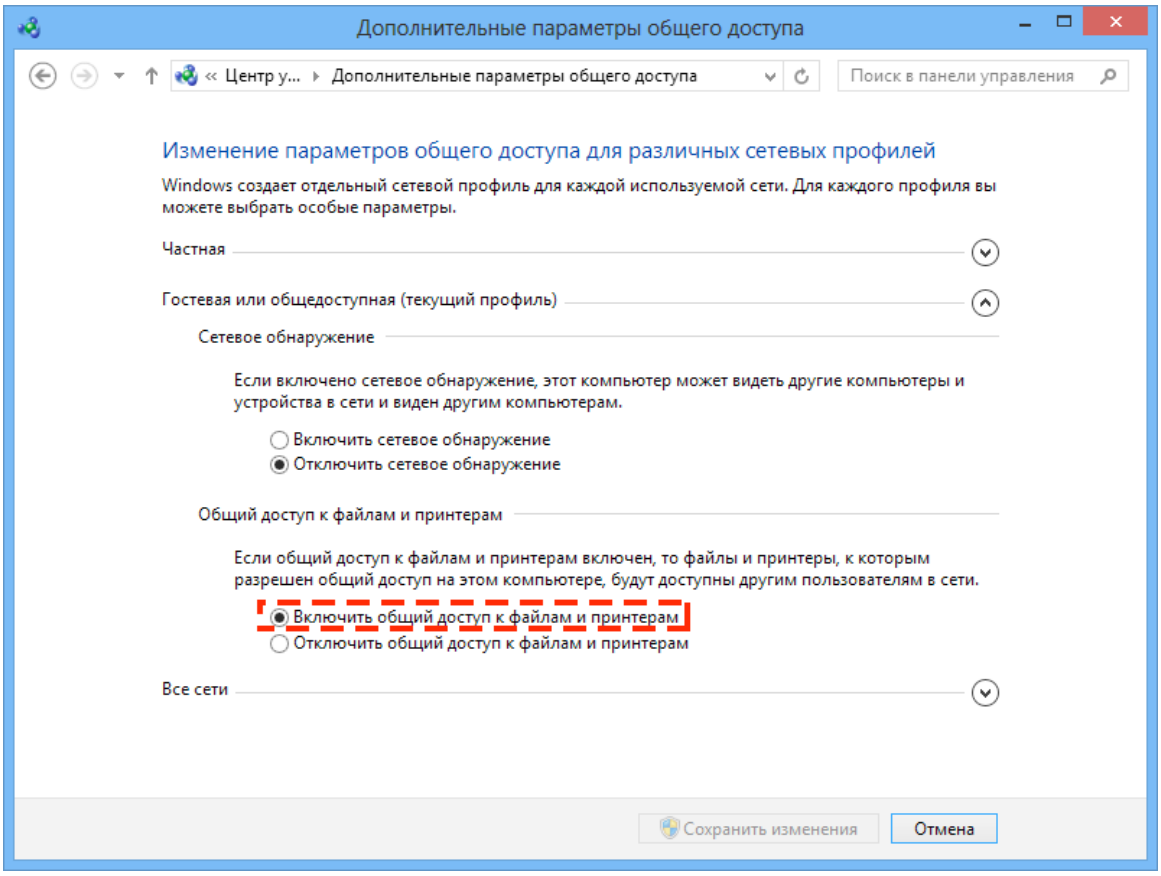
Если вы настраиваете Windows 2008 или Windows 2008 R2, опцию **Включить сетевое обнаружение** использовать не нужно.

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Нажмите на кнопки **Windows + X**.



В открывшемся контекстном меню выберите пункт **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа**. В общем сетевом профиле выберите пункт **Включить общий доступ к файлам и принтерам**.



Нажмите на кнопку **Сохранить изменения**.

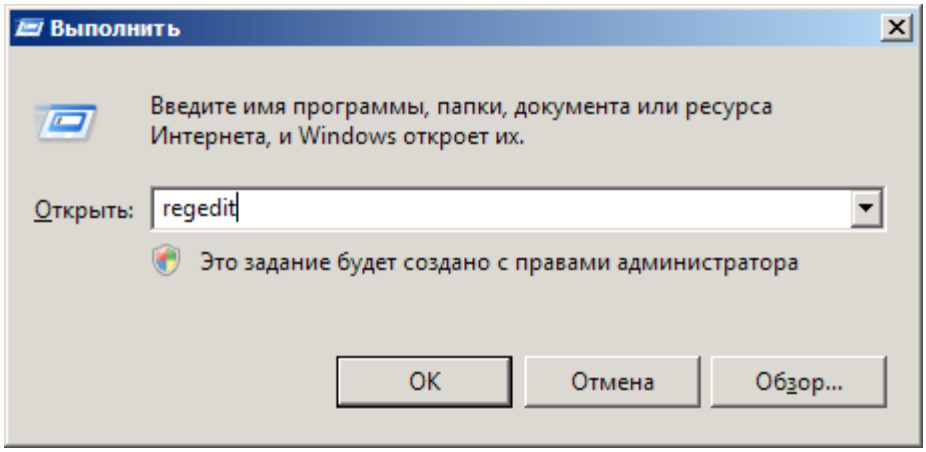
Настройка системы контроля учетных записей (UAC)

Ограничения должны быть отключены, если станция работает под управлением Windows Vista или более поздней операционной системы. Если вы работаете под встроенным аккаунтом администратора, то данную настройку проводить не нужно.

- **Windows Vista**

На всех станциях, подлежащих проверке, откройте редактор реестра операционной системы.

Нажмите на клавиши **Windows** + **R**.

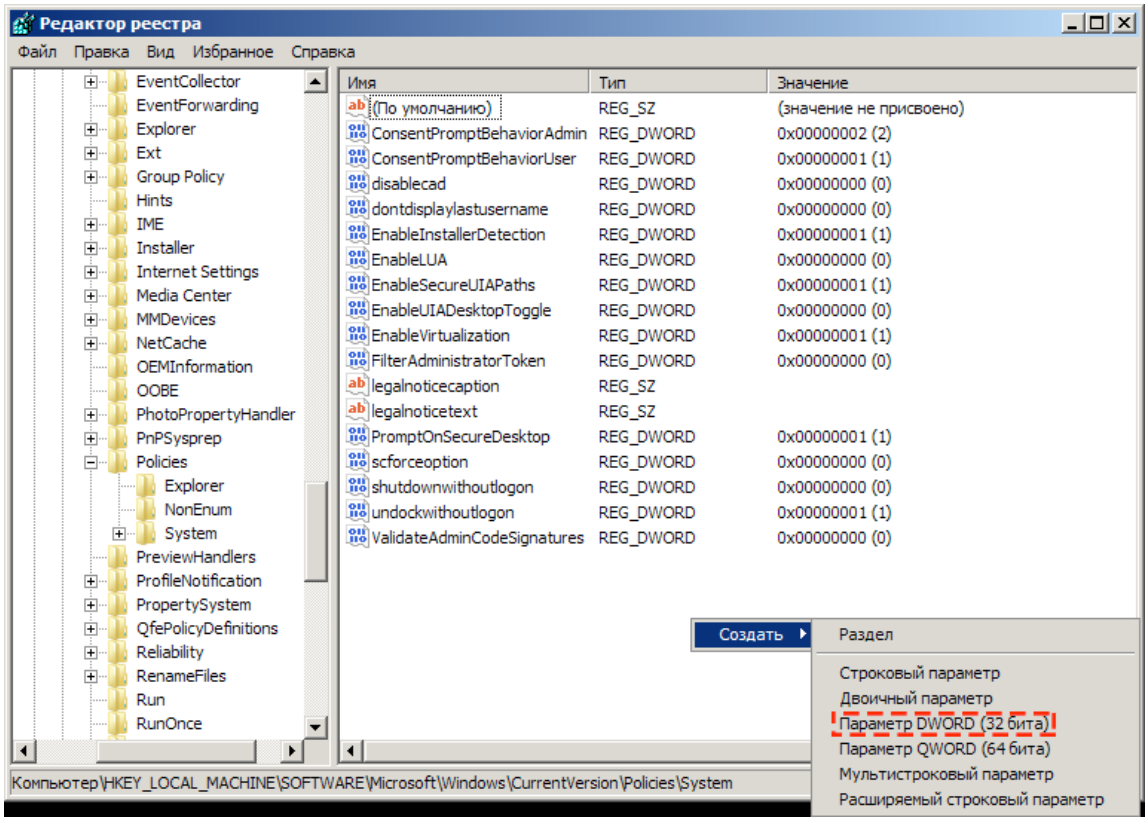


В открывшемся окне введите Regedit. Откроется окно редактора реестра Windows. Откройте ветку

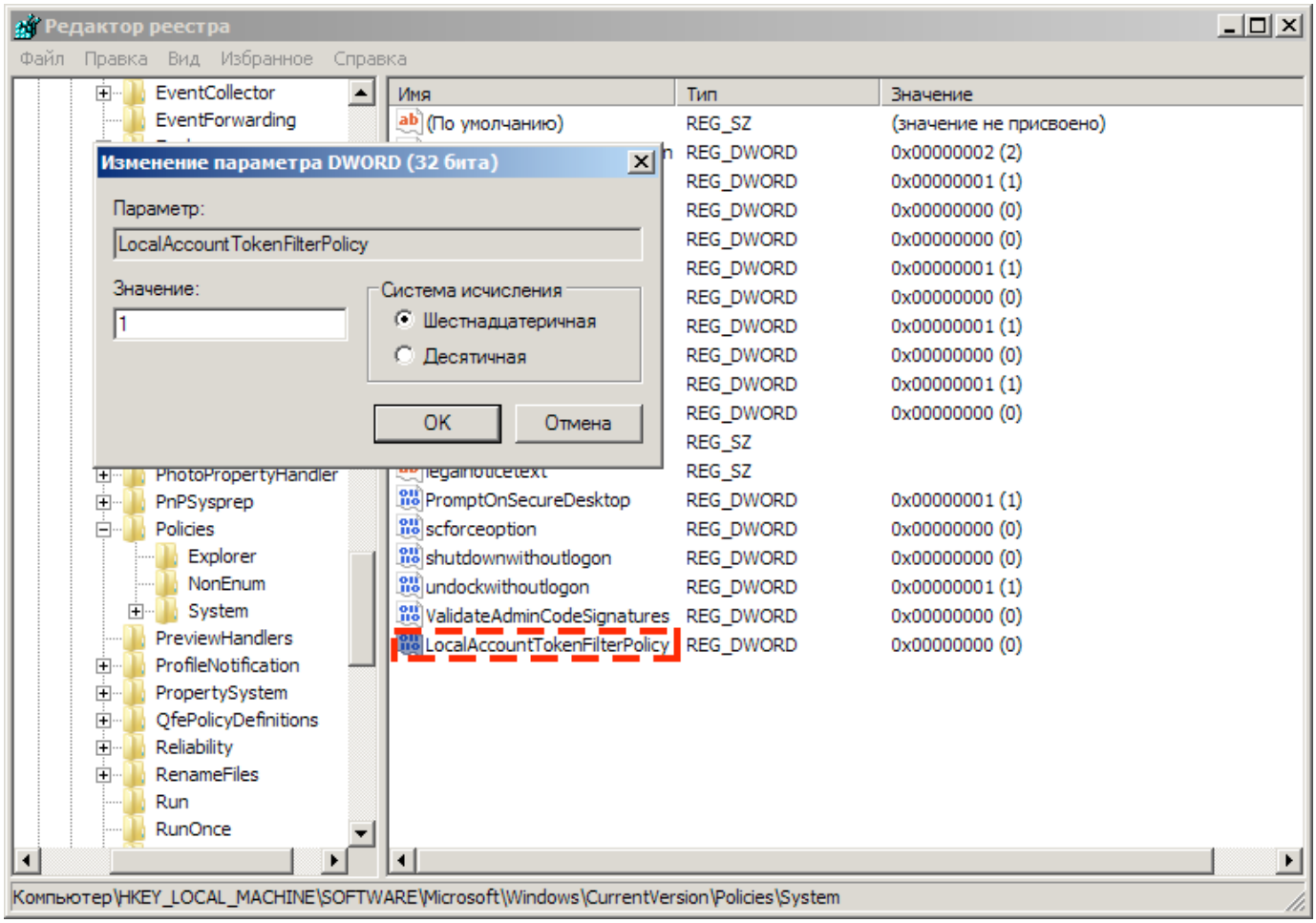
[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

Если в данной ветке отсутствует ключ **LocalAccountTokenFilterPolicy**, создайте его.

Перейдите в правую часть окна редактора реестра Windows, нажмите правую клавишу мыши и выберите в контекстном меню опцию **Создать → Параметр DWORD 32 бита**.



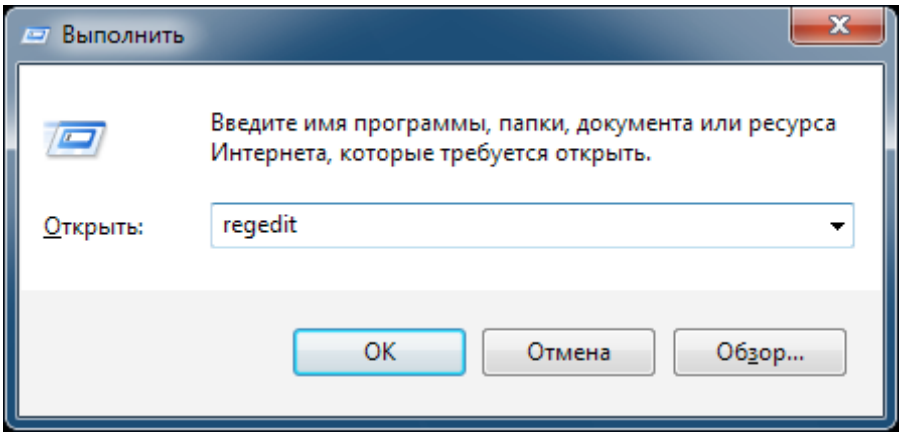
Установите название параметра LocalAccountTokenFilterPolicy. Дважды щелкните по созданному параметру левой клавишей мыши. Откроется окно **Изменение параметра DWORD**. Установите значение, равное 1, и нажмите на кнопку **ОК**.



Закройте редактор реестра Windows. Сделайте остальные настройки и перезагрузите компьютер.

- **Windows 7**

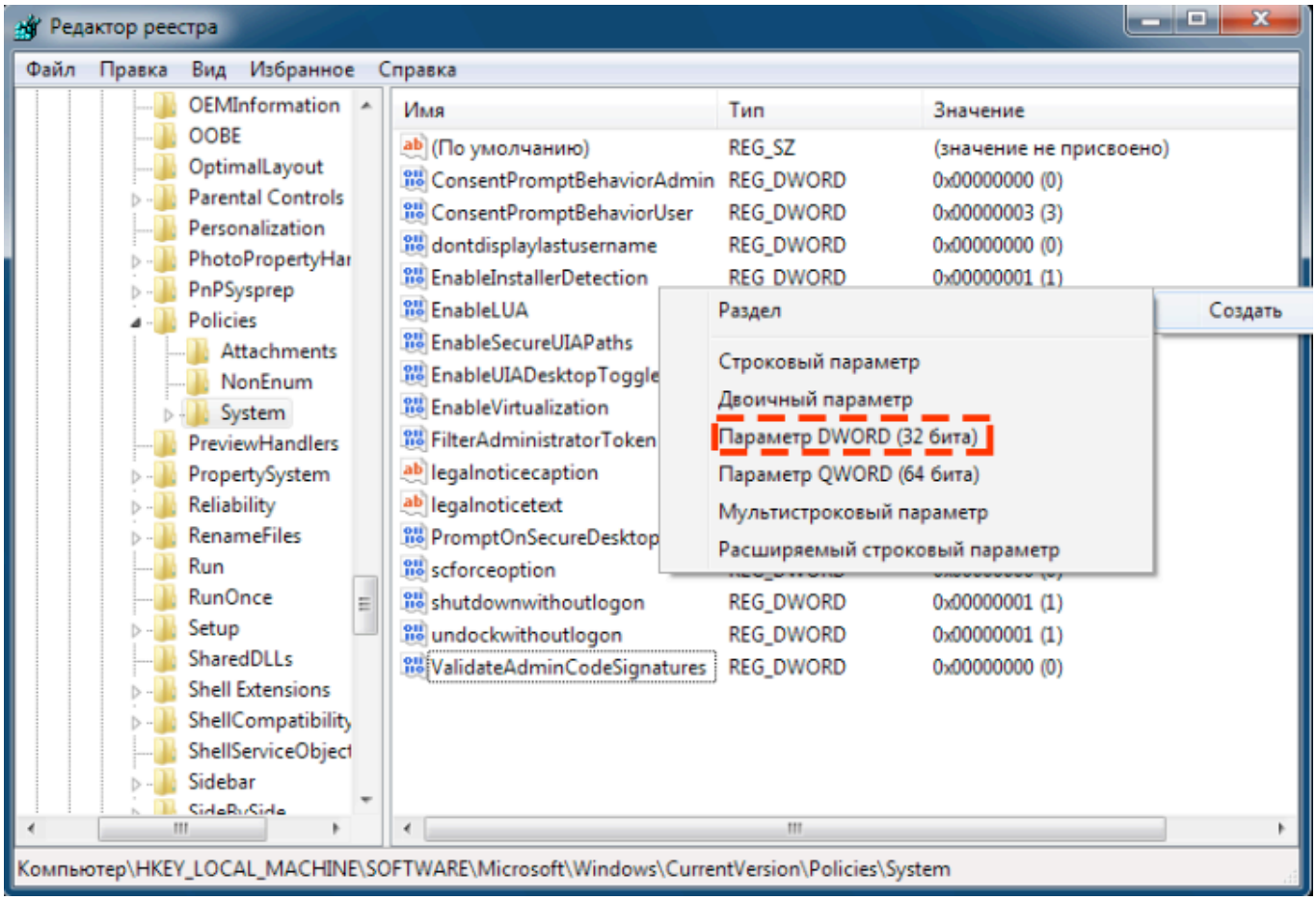
Нажмите на клавиши **Windows** + **R**.



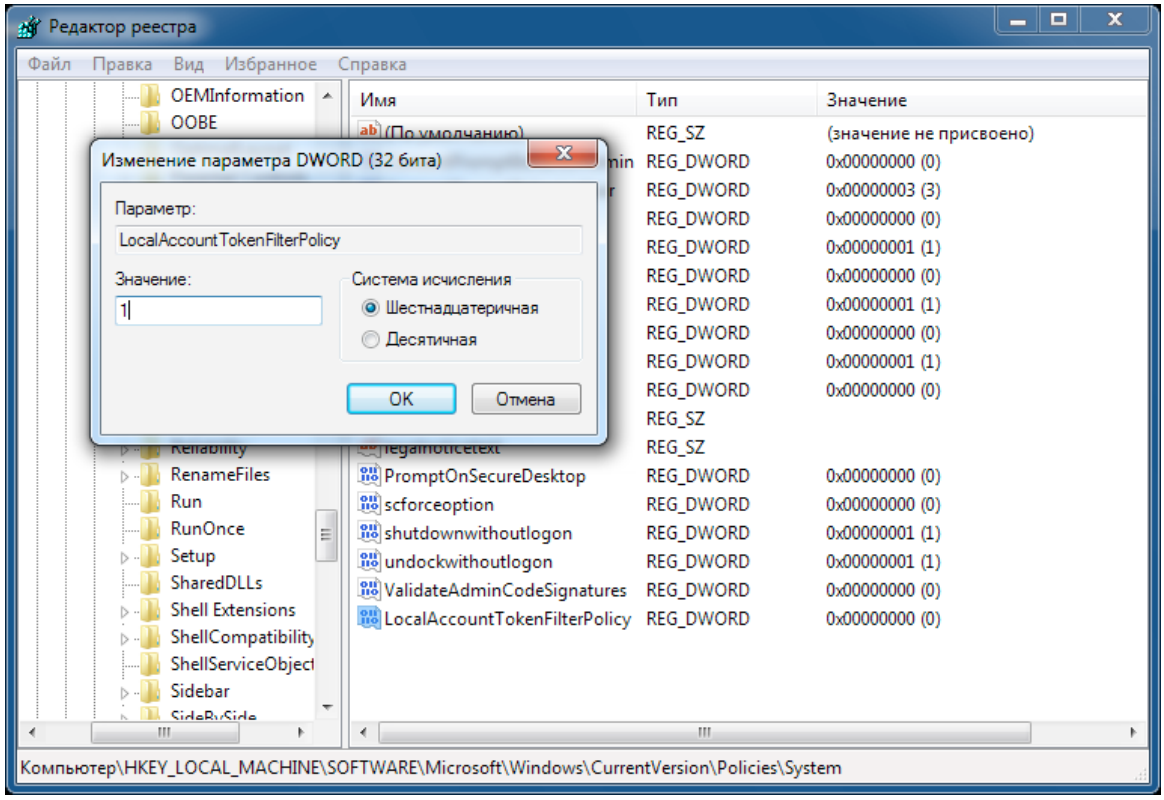
В открывшемся окне введите Regedit. Откроется окно редактора реестра Windows. Откройте ветку

[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

Перейдите в правую часть окна редактора реестра Windows, нажмите правую клавишу мыши и выберите в контекстном меню пункт **Создать параметр DWORD 32 бита**.



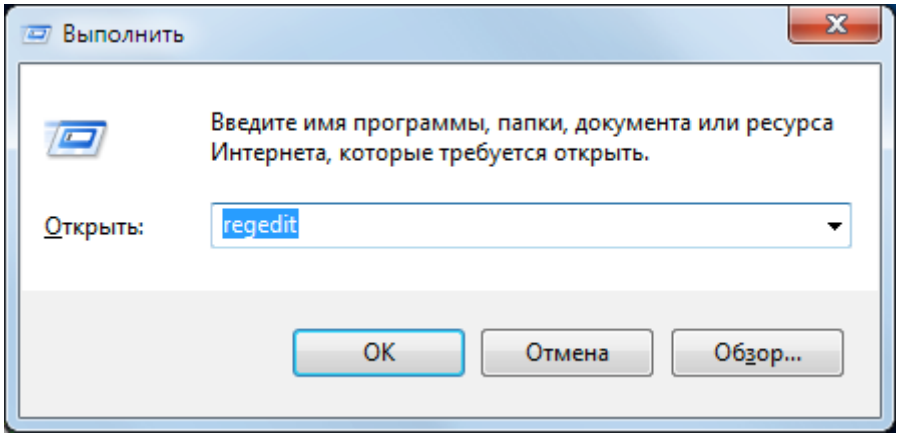
Установите название параметра LocalAccountTokenFilterPolicy. Дважды щелкните по созданному параметру левой клавишей мыши. Откроется окно **Изменение параметра DWORD**. Установите значение, равное единице, и нажмите **ОК**.



Закройте редактор реестра. Выполните остальные настройки и перезагрузите компьютер.

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

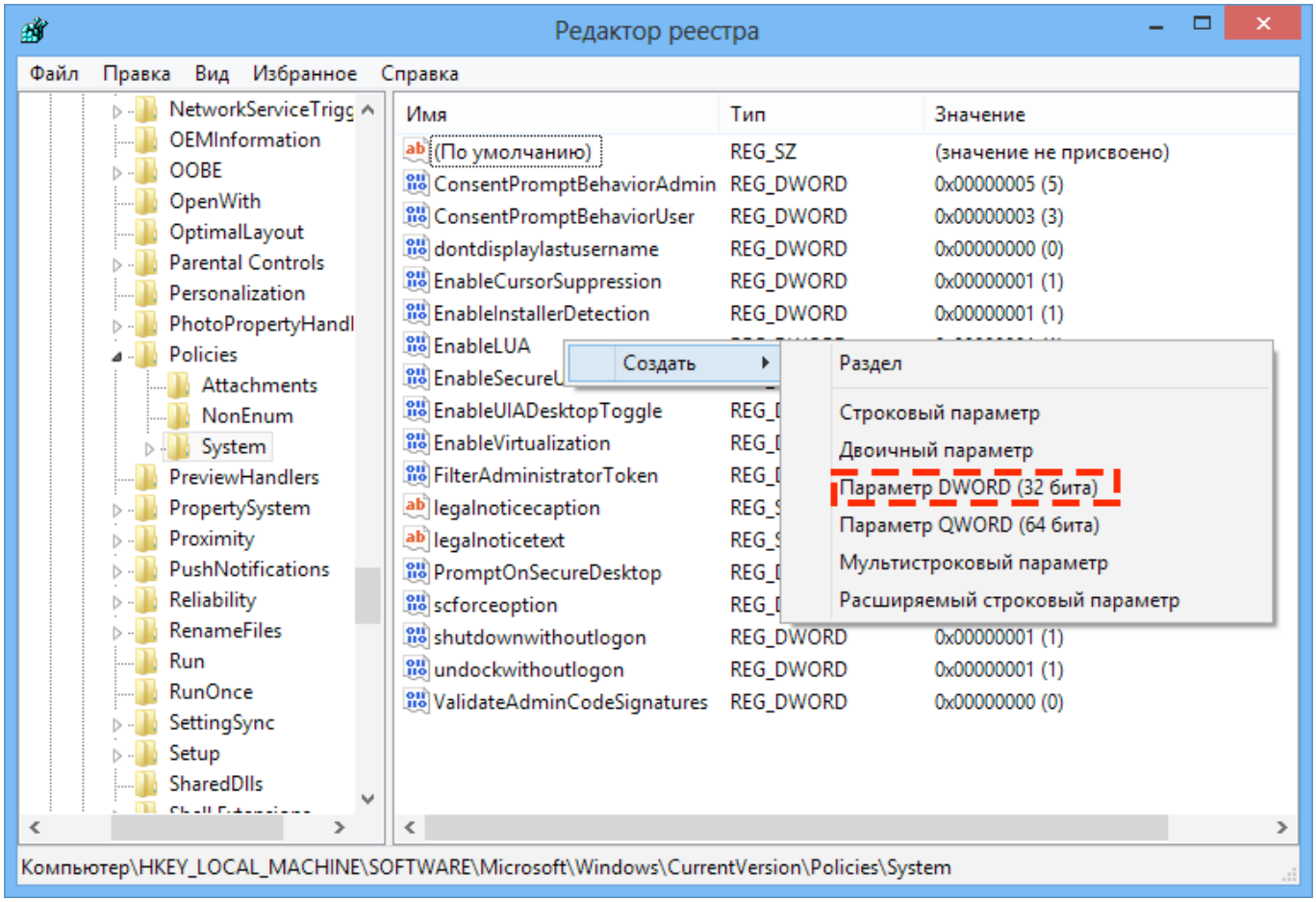
Нажмите на клавиши **Windows** + **R**.



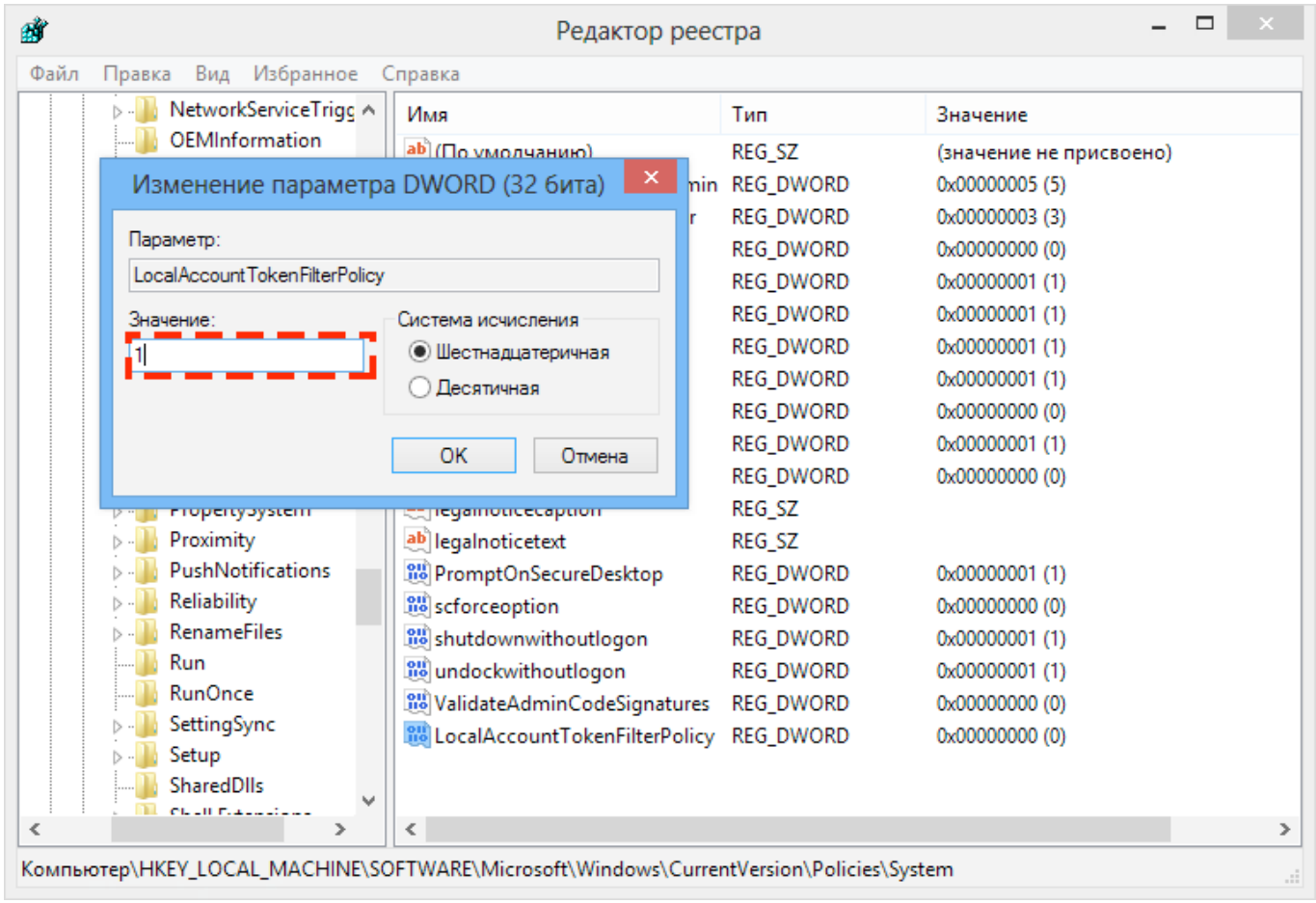
В открывшемся окне введите Regedit. Откроется окно редактора реестра Windows. Откройте ветку

[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

Перейдите в правую часть окна редактора реестра Windows, нажмите правую клавишу мыши и выберите в контекстном меню пункт **Создать параметр DWORD 32 бита**.



Установите название параметра LocalAccountTokenFilterPolicy. Дважды щелкните по созданному параметру левой клавишей мыши. Откроется окно **Изменение параметра DWORD**. Установите значение, равное единице, и нажмите **ОК**.



Закройте редактор реестра. Выполните остальные настройки (пункты 2–6) и перезагрузите компьютер.

Настройка брандмауэра

Если для защиты удаленного компьютера используется брандмауэр, необходимо провести дополнительные настройки, описанные ниже.

При использовании брандмауэра Windows в его настройках перейдите на вкладку **Дополнительные параметры**, выберите **Правила для входящих подключений** и включите следующие исключения: **Служба входа в сеть (NP-In)** и **Общий доступ к файлам и принтерам (SMB-In)**.

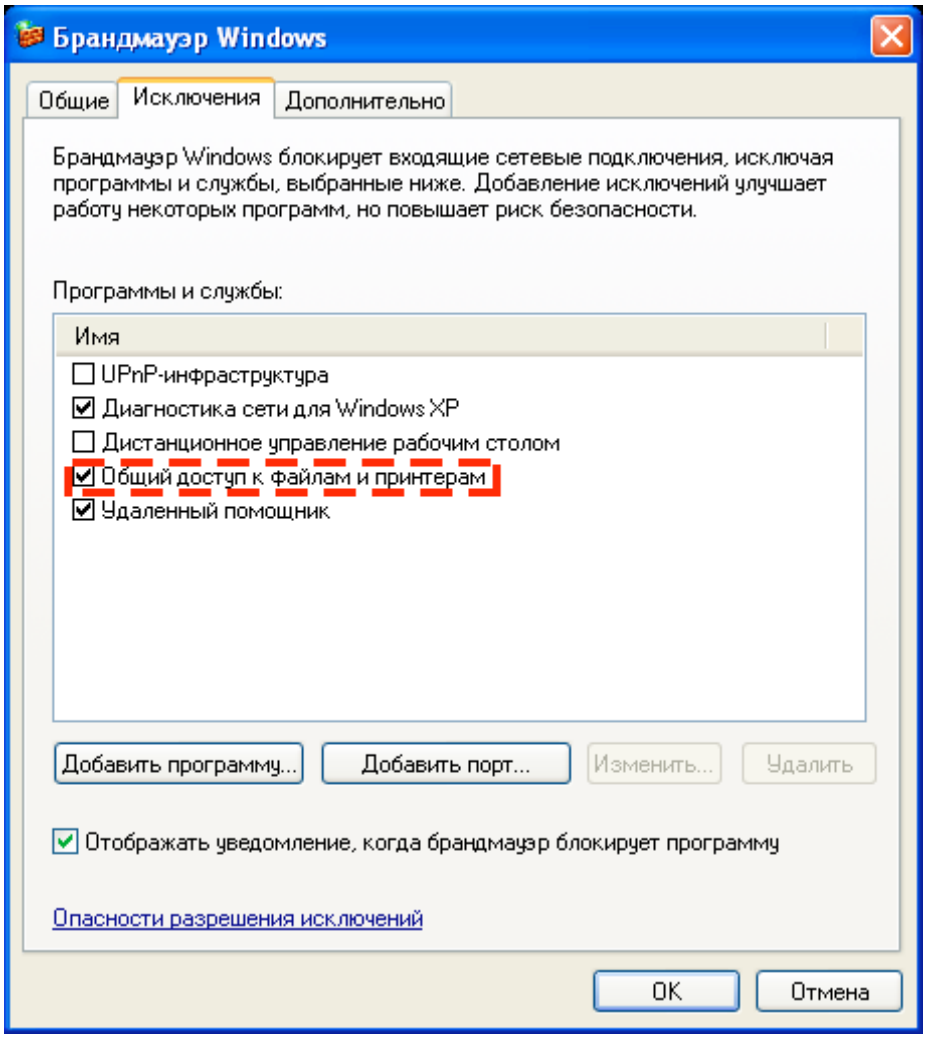
Исключения должны быть включены для профиля брандмауэра **Private**. Если станция находится в домене, исключения должны быть включены для профиля **Domain**.

При использовании других брандмауэров необходимо открыть порт 445.

Далее рассмотрим пример настроек **Общего доступа к файлам и принтерам**, если применяется брандмауэр Windows.

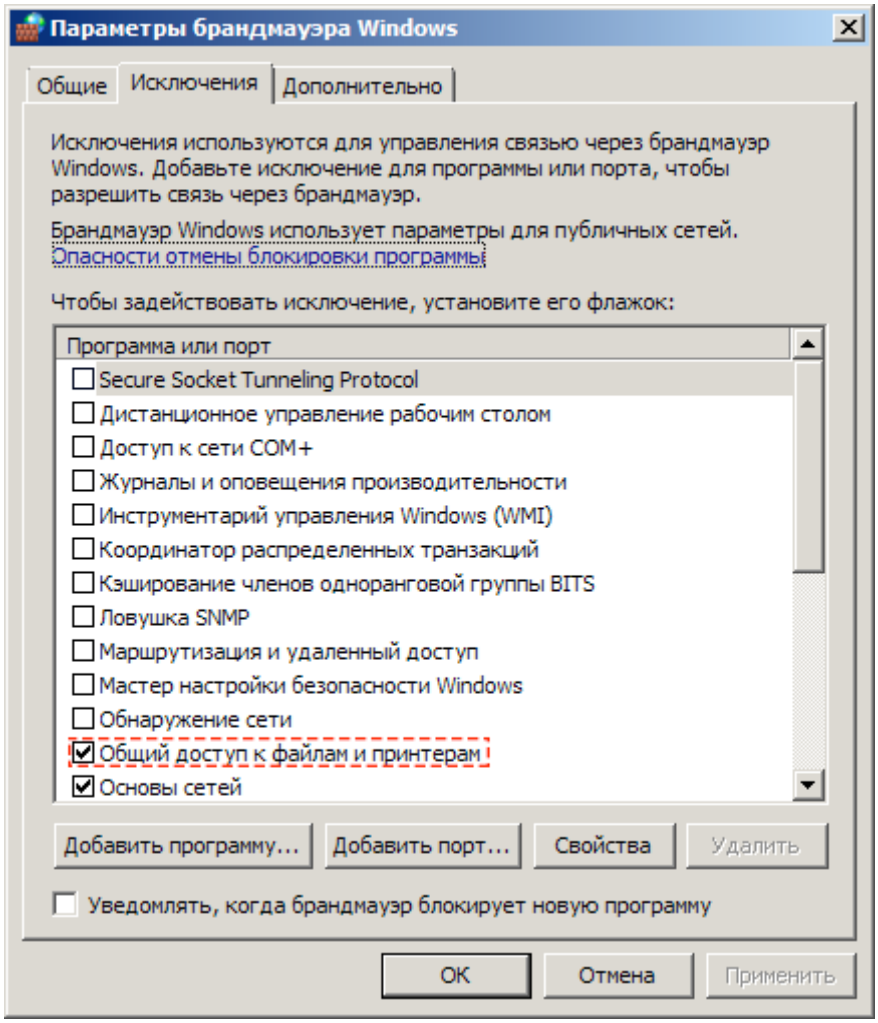
- **Windows XP, Windows 2003**

Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления** → **Брандмауэр Windows**. Откроется окно **Брандмауэр Windows**. Перейдите на вкладку **Исключения**. Включите опцию **Общий доступ к файлам и принтерам**. Нажмите на кнопку **ОК**.



- **Windows Vista, Windows Server 2008**

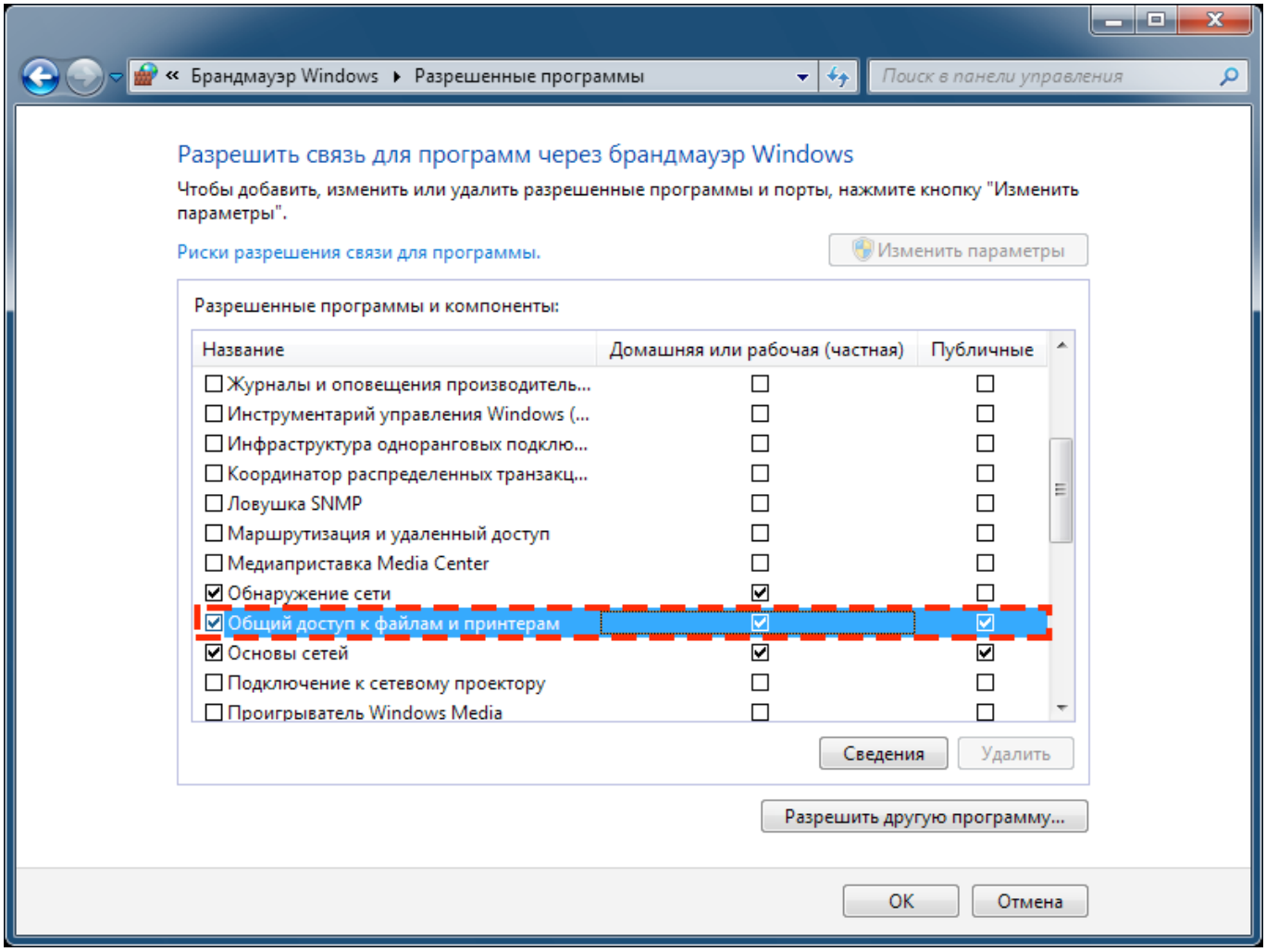
Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Безопасность → Брандмауэр Windows**. Перейдите по ссылке **Включение и отключение брандмауэра Windows**. В открывшемся окне **Параметры брандмауэра Windows** перейдите на вкладку **Исключения**. Поставьте флаг **Общий доступ к файлам и принтерам**.



Нажмите на кнопку **ОК**.

- **Windows 7, Windows Server 2008 R2**

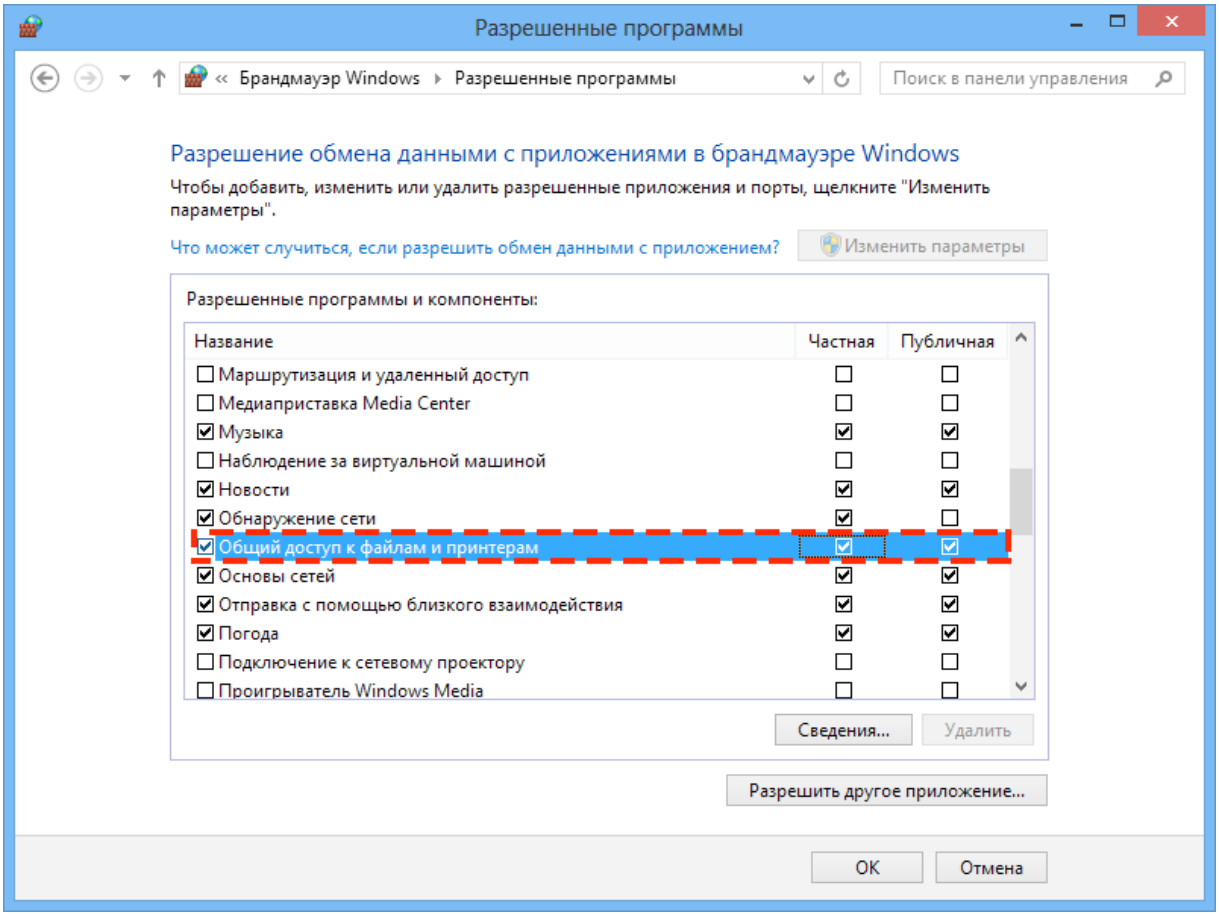
Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Система и безопасность → Брандмауэр Windows → Разрешить запуск программы или компонента через брандмауэр Windows**. Нажмите на кнопку **Изменить параметры**. Поставьте флаги **Общий доступ к файлам и принтерам**.



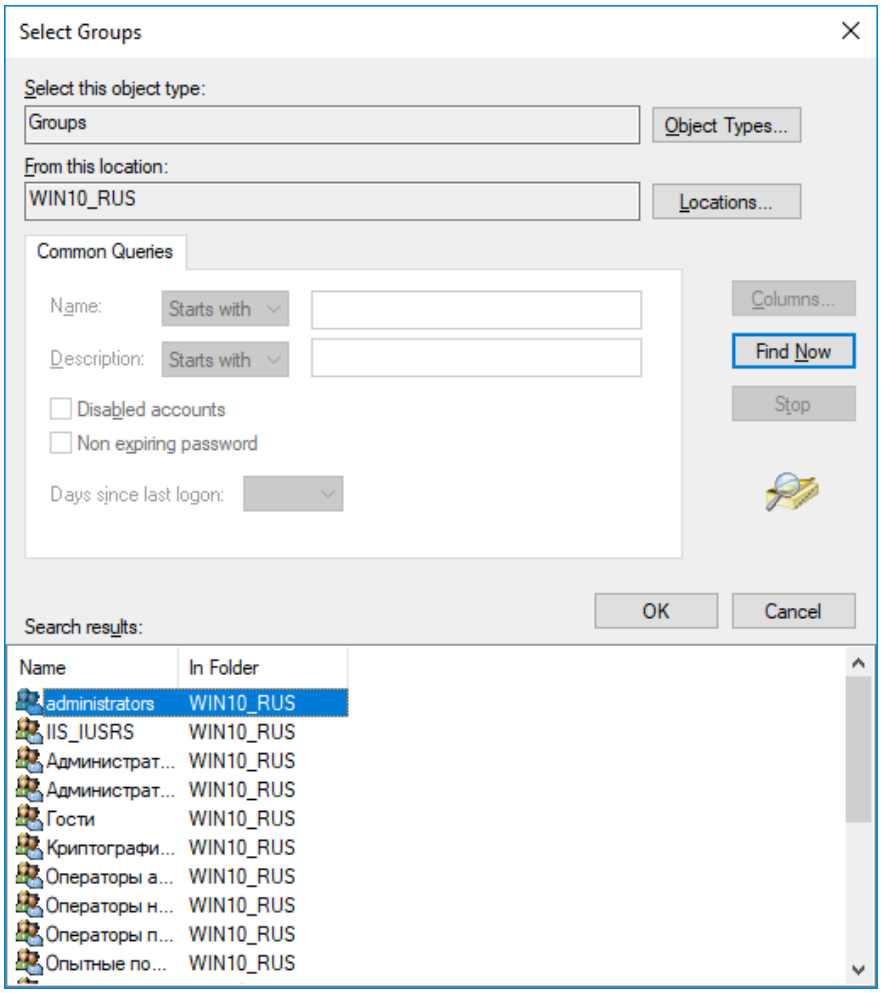
Нажмите на кнопку **ОК**.

- **Windows 8, 10, Windows 8.1 Windows Server 2012**

Нажмите на кнопки **Windows + X**. В открывшемся контекстном меню выберите пункт **Панель управления → Система и безопасность → Брандмауэр Windows → Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows**. Нажмите на кнопку **Изменить параметры**. Поставьте флаги **Общий доступ к файлам и принтерам**.



Если у вас установлен иной брандмауэр, данная группа настроек будет заблокирована.



Нажмите на кнопку **ОК**.

Настройка локальной политики безопасности

Для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности.

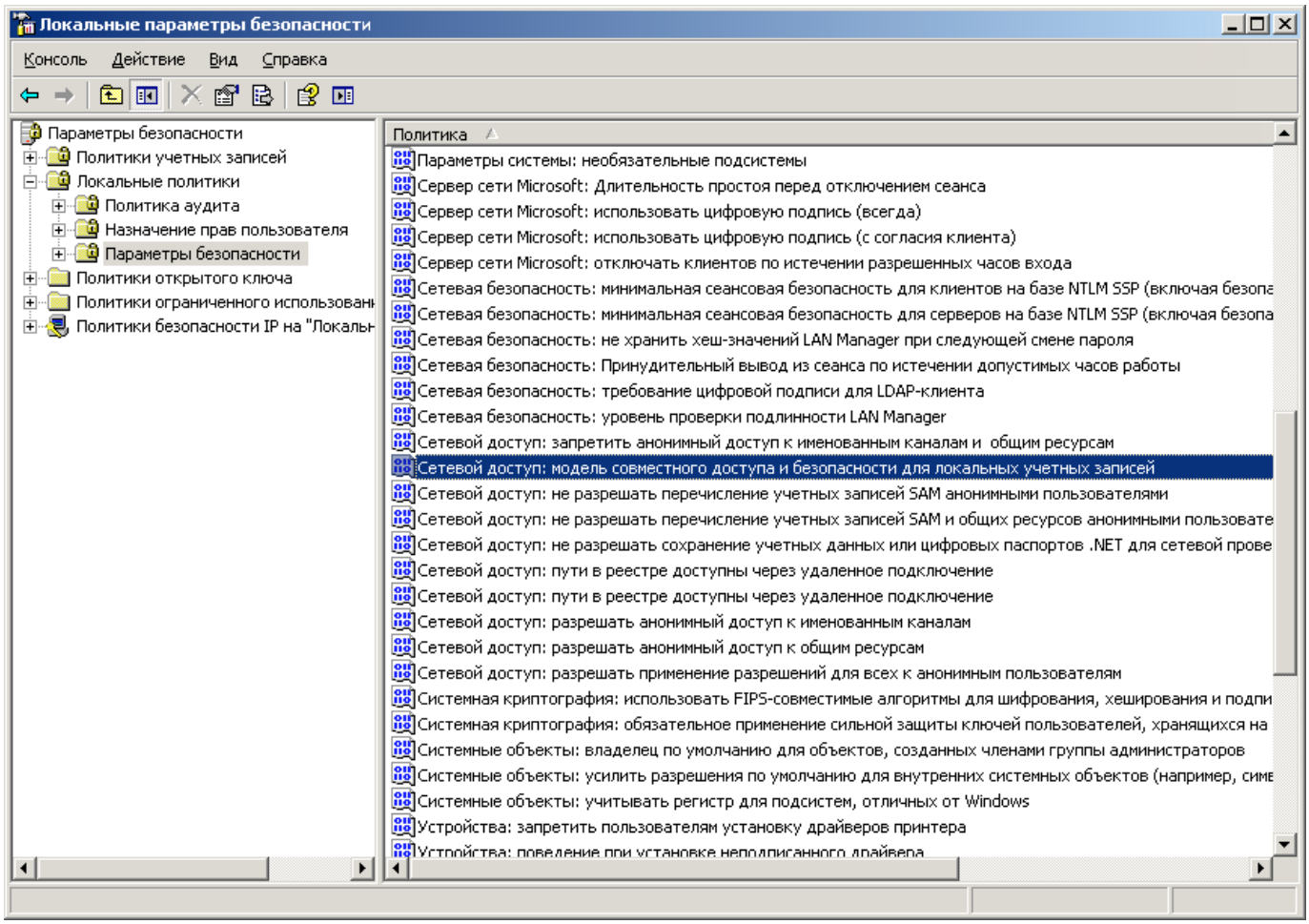
По умолчанию подключение к удаленному компьютеру не может быть установлено, если используемая учетная запись содержит пустой пароль. Чтобы подключиться, задайте непустой пароль.

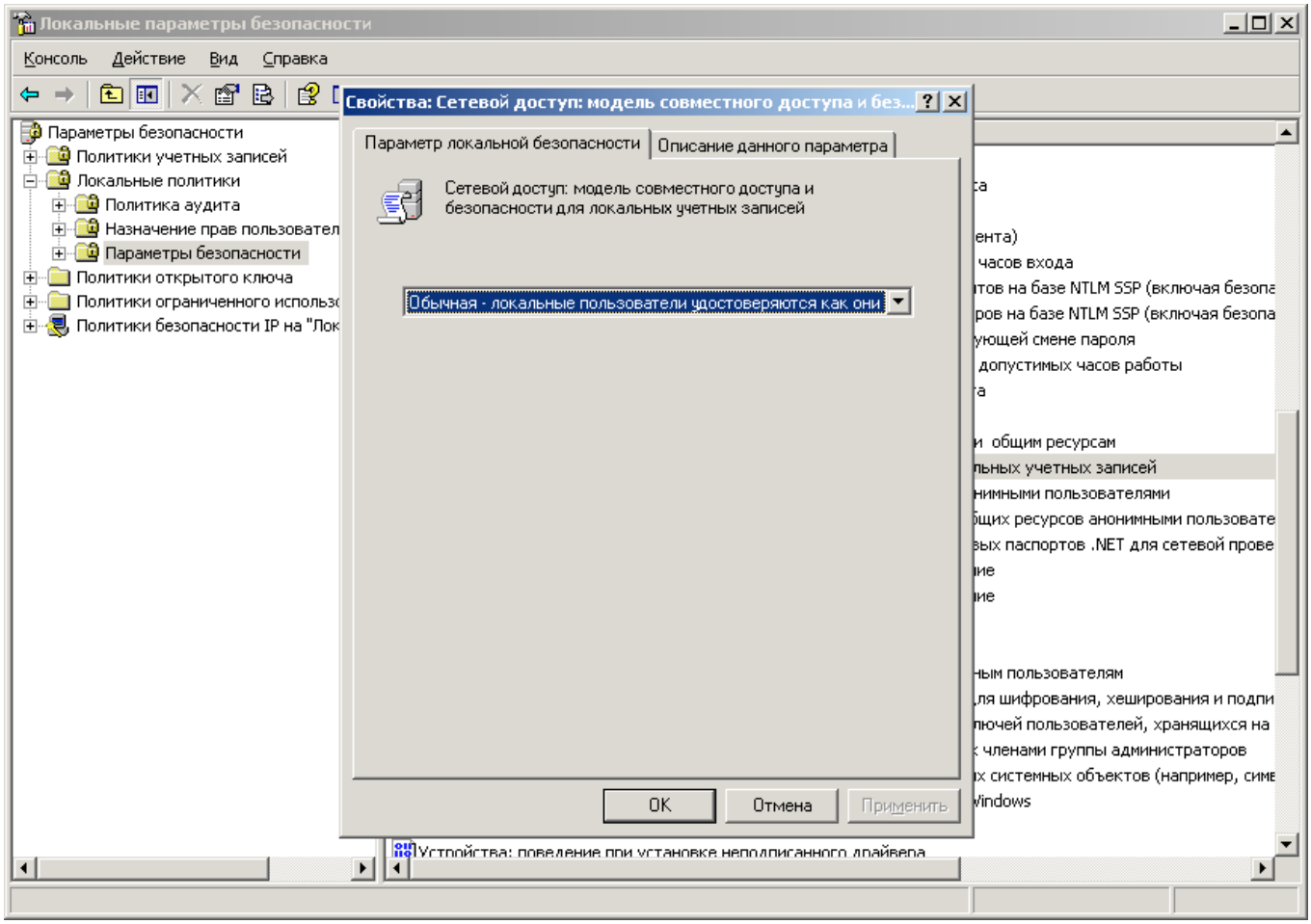
- **Windows XP, Windows 2003**

Перейдите в **Панель управления → Администрирование** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**) **→ Локальная политика безопасности → Локальные политики → Параметры безопасности**.

Наведите курсор мыши на политику **Сетевой доступ: модель совместного доступа для локальных учетных записей** и дважды щелкните левой клавишей мыши. Откроется окно **Свойства**. Задайте значение **Обычная — локальные пользователи удостоверяются как они сами**.

Для запуска утилиты по настройке локальных политик безопасности вы также можете набрать в поле поиска ОС Windows команду **secpol.msc** и нажать клавишу **ENTER**.





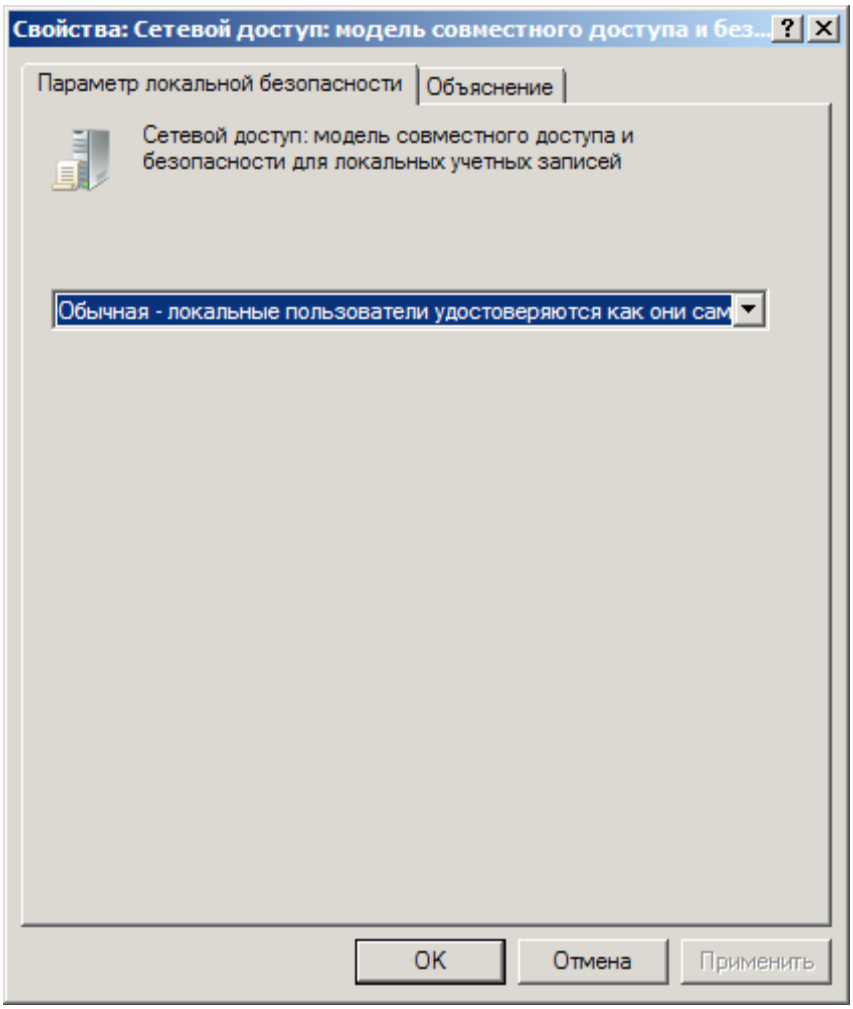
Последовательно нажмите на кнопки **Применить** и **ОК**. Закройте оснастку **Локальные параметры безопасности**.

Выделите курсором мыши сетевое подключение, нажмите правую клавишу мыши. Появится контекстное меню, выберите в нем пункт **Свойства**. Откроется окно настроек сетевого подключения.

Нажмите на кнопку **ОК**.

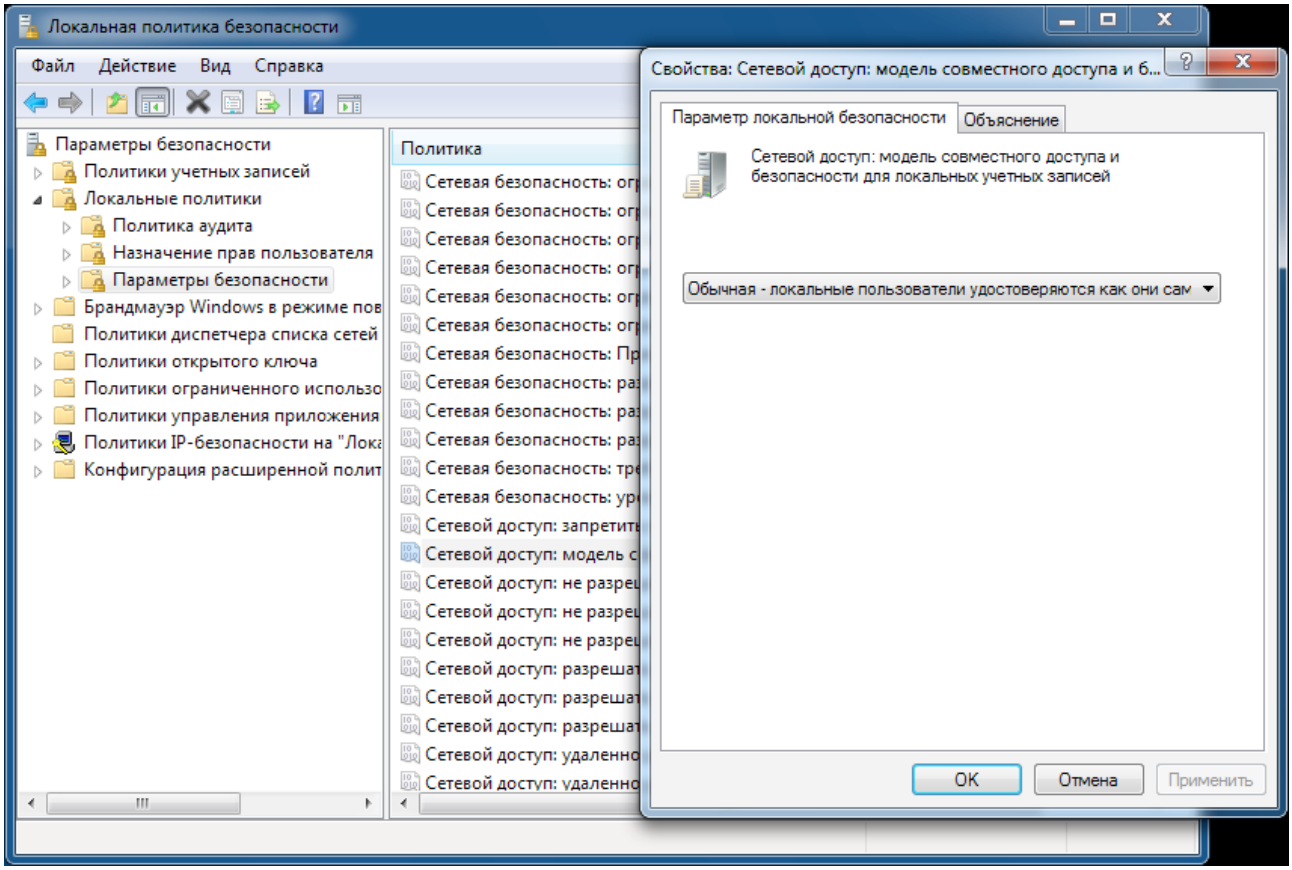
- **Windows Vista, Windows Server 2008**

Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Система и ее обслуживание → Администрирование → Локальная политика безопасности → Локальные политики → Параметры безопасности**. Выделите курсором мыши политику **Сетевой доступ: модель совместного доступа для локальных учетных записей**. Дважды щелкните по ней левой клавишей мыши. Откроется окно **Свойства**. Задайте значение **Обычная — локальные пользователи удостоверяются как они сами**, и нажмите на кнопку **ОК**.



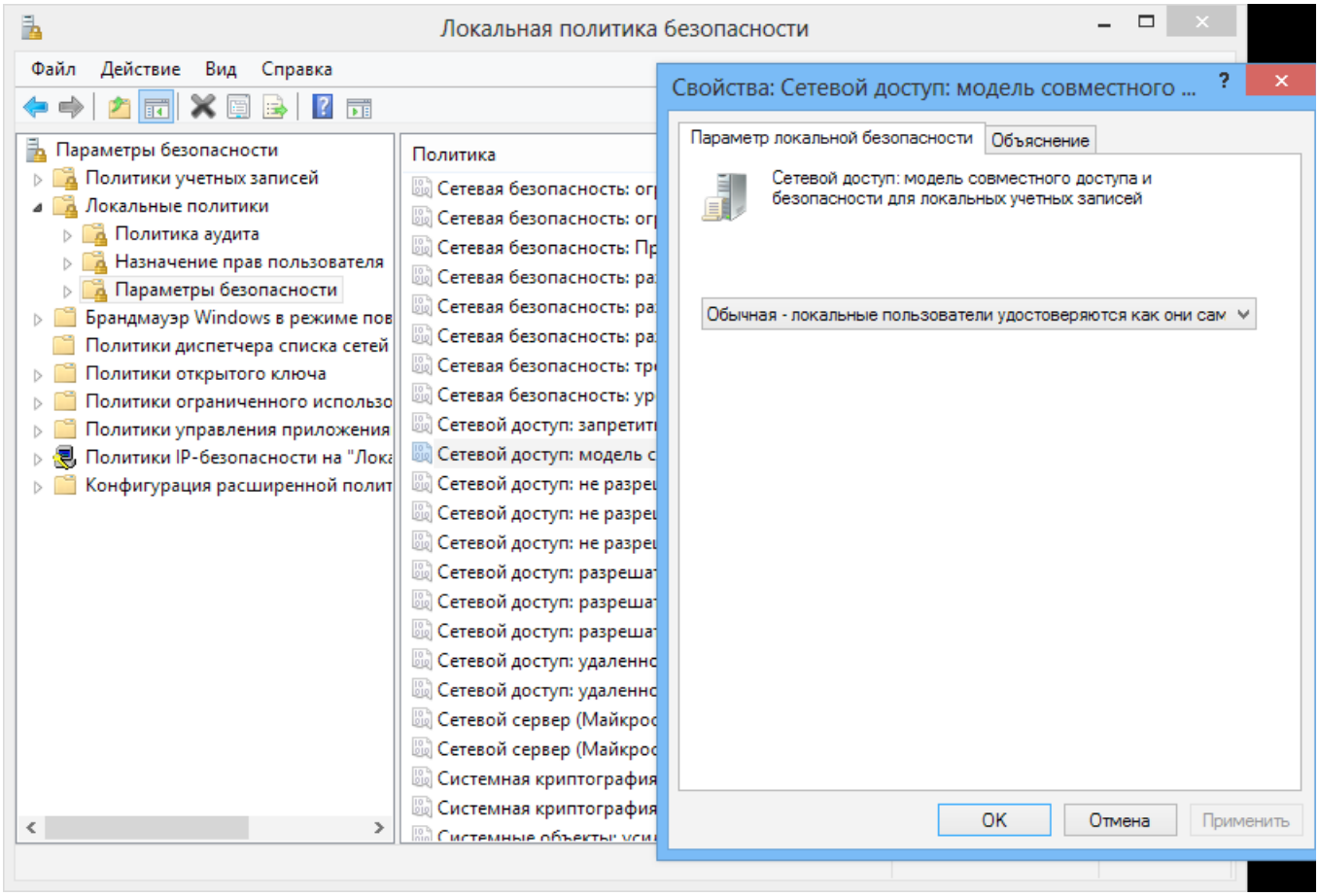
- **Windows 7, Windows Server 2008 R2**

Нажмите на кнопку **Пуск** и перейдите по меню **Панель управления → Система и безопасность → Администрирование → Локальная политика безопасности → Локальные политики → Параметры безопасности**. Выберите политику **Сетевой доступ: модель совместного доступа для локальных учетных записей**. Дважды щелкните по ней левой клавишей мыши. Откроется окно **Свойства**. Задайте значение **Обычная — локальные пользователи удостоверяются как они сами**, и нажмите на кнопку **ОК**.



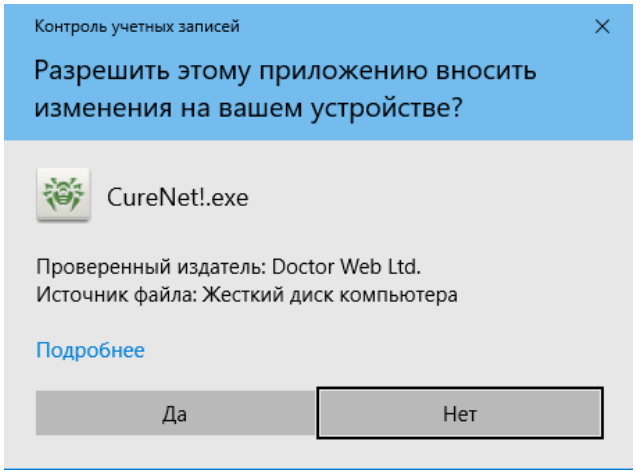
- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Нажмите на кнопки **Windows + X**. В открывшемся контекстном меню выберите пункт **Панель управления → Система и безопасность → Администрирование → Локальная политика безопасности → Локальные политики → Параметры безопасности**. Выберите политику **Сетевой доступ: модель совместного доступа для локальных учетных записей**. Дважды щелкните по ней левой клавишей мыши. Откроется окно **Свойства**. Задайте значение **Обычная — локальные пользователи удостоверяются как они сами**, и нажмите на кнопку **ОК**.



Запуск Dr.Web CureNet!

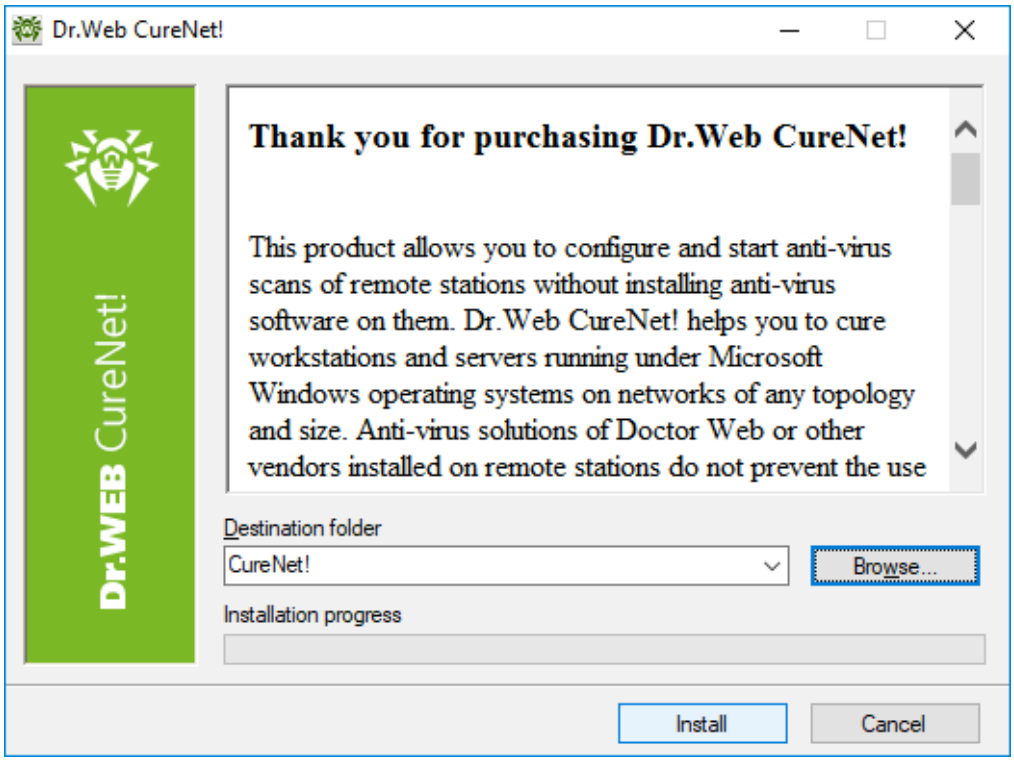
1. Запустите полученный вами дистрибутив CureNet!.exe, при необходимости подтвердив его запуск.



Внимание! Процедура последующих запусков Dr.Web CureNet! описана ниже.

Внимание! Хотя Dr.Web CureNet! совместим с антивирусными продуктами других производителей, рекомендуется для ускорения процесса проверки запретить их работу на время работы Dr.Web CureNet!

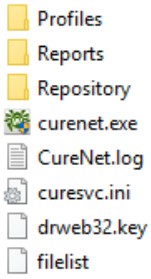
2. Для продолжения нажмите на кнопку **Install**.



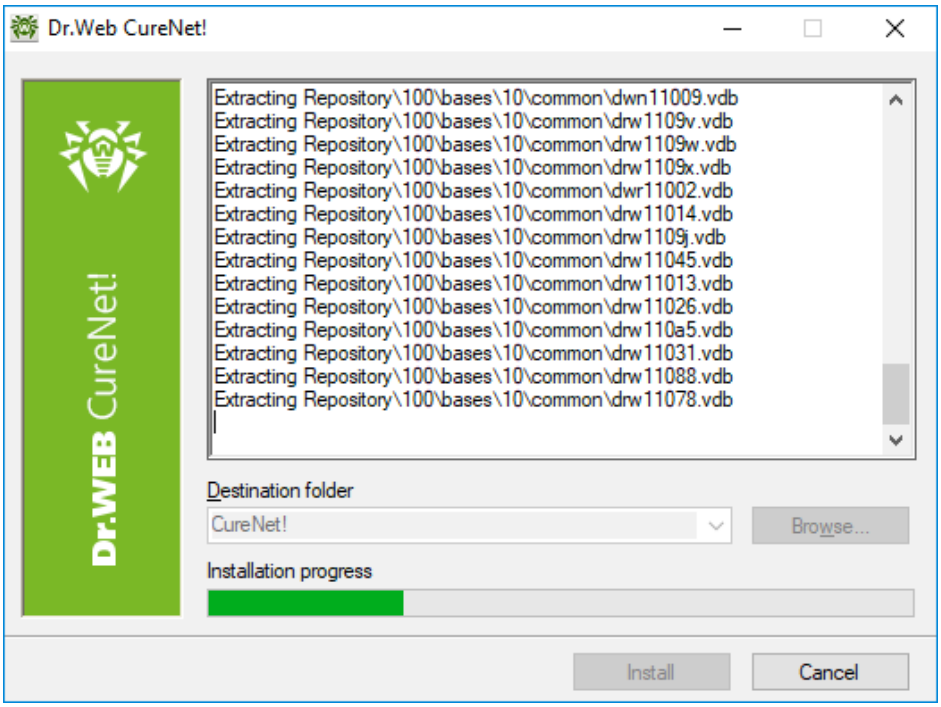
3. Если вы хотите сохранить файлы Dr.Web CureNet! для дальнейшего использования в папку, отличную от папки по умолчанию, выберите ее, нажав кнопку **Browse**.

CureNet!.exe представляет собой самораспаковывающийся архив, в связи с чем продукт не требует инсталляции. Вам необходимо только выбрать место, куда будут распакованы файлы из этого архива. Имя папки по умолчанию — CureNet!, но вы всегда можете определить любое другое имя. Если вы распакуете архив на USB flash или любое подобное устройство. drive, вы всегда будете иметь Dr.Web CureNet! под рукой на случай возникновения непредвиденных ситуаций.

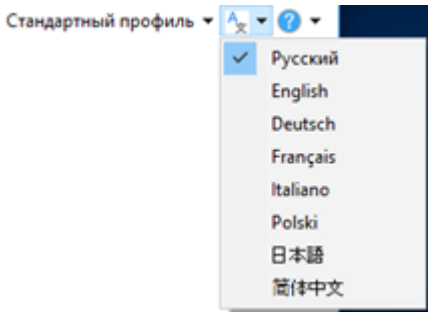
В созданной в результате распаковки папке будут содержаться файлы репозитория продукта и ключевой файл



Для продолжения установки нажмите кнопку **Install**.

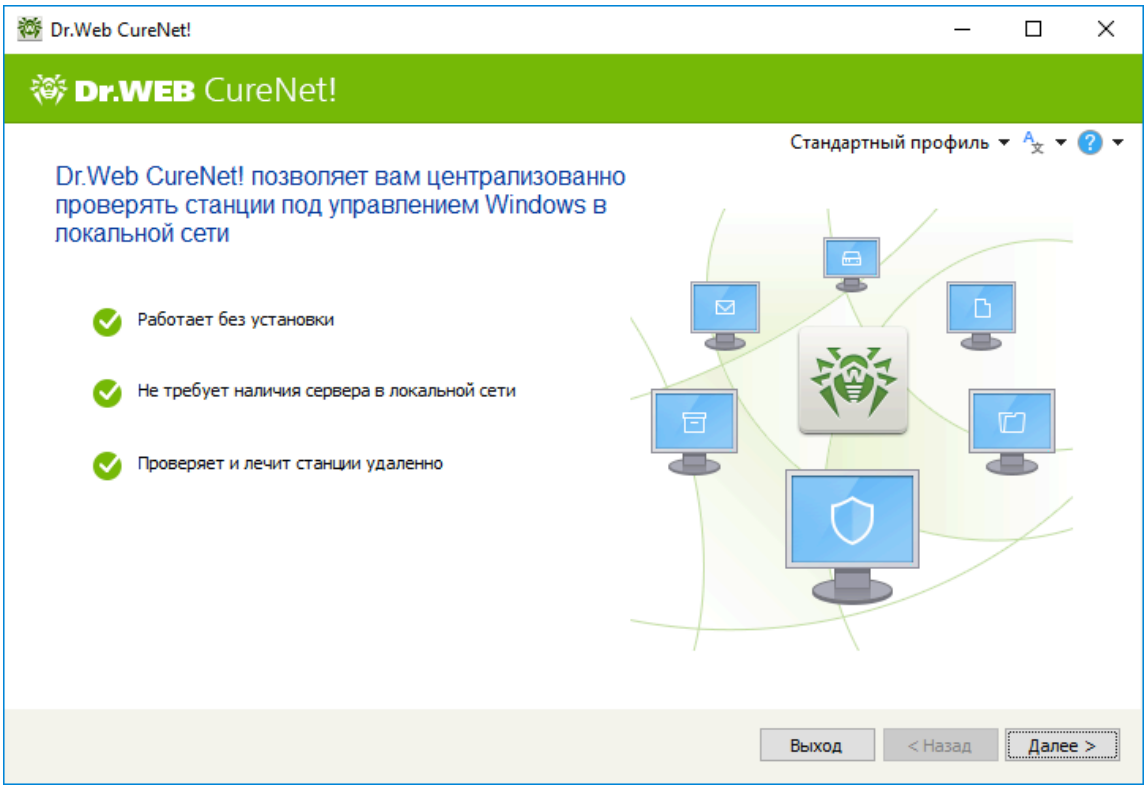


4. В открывшемся окне программы вы можете выбрать язык локализации, нажав кнопку  в верхнем правом углу.



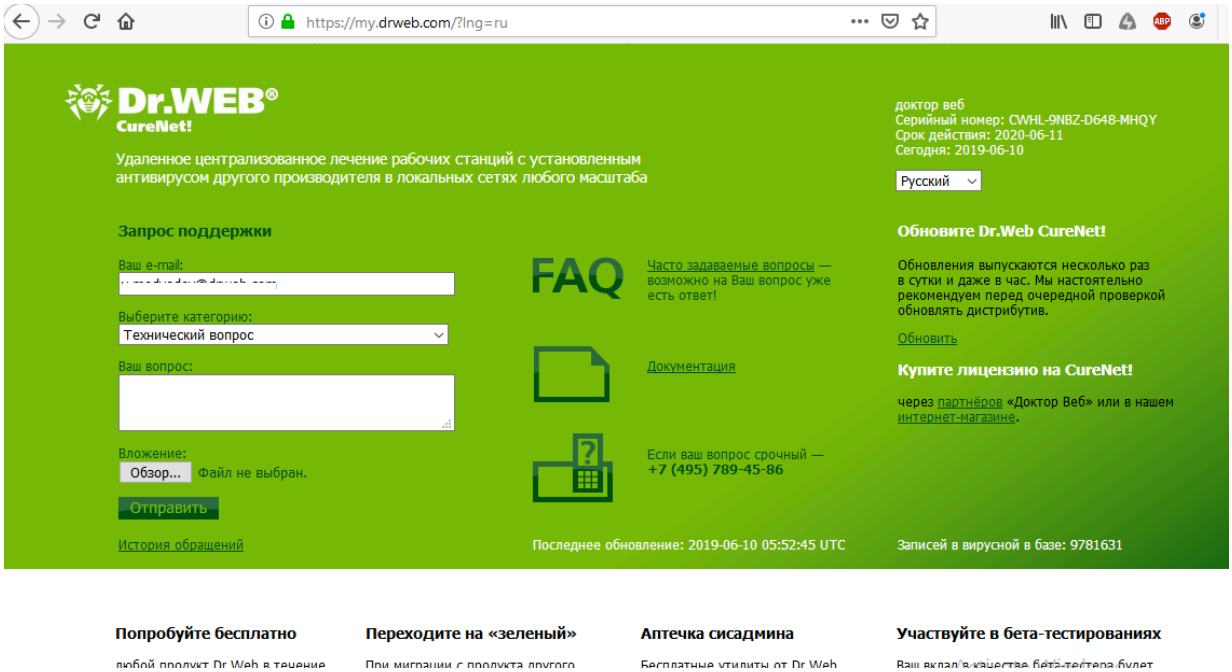
Внимание! Если вы используете русифицированную версию операционной системы, убедитесь в том, что на ней установлены все необходимые для отображения русских символов компоненты.

В том случае, если у вас имеются сохраненные ранее настройки сканирования, вы можете загрузить их, нажав кнопку **Стандартный профиль** в верхнем правом углу.

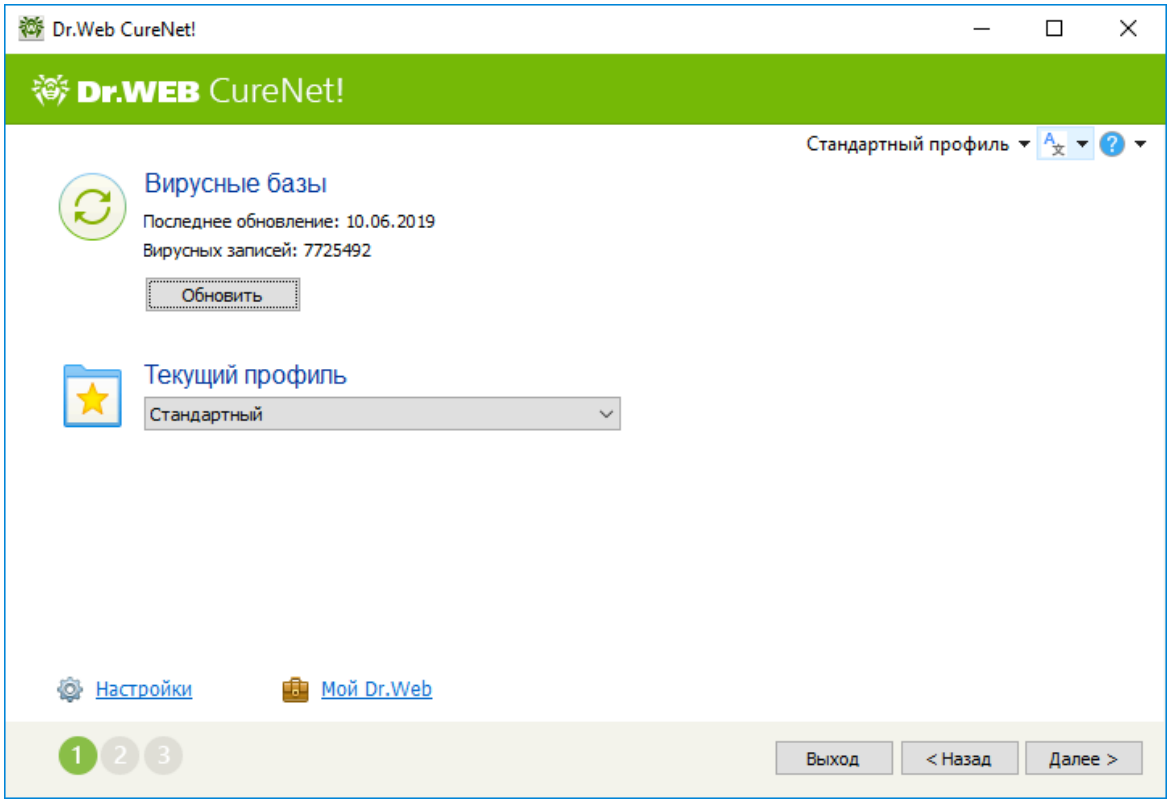


В случае возникновения каких-либо вопросов нажмите кнопку . Выбрав **Помощь** в контекстном меню, вы можете ознакомиться с Руководством пользователя. Выбрав **Мой Dr.Web**, вы переходите на вашу персональную страницу, где вы можете создать запрос в техподдержку.

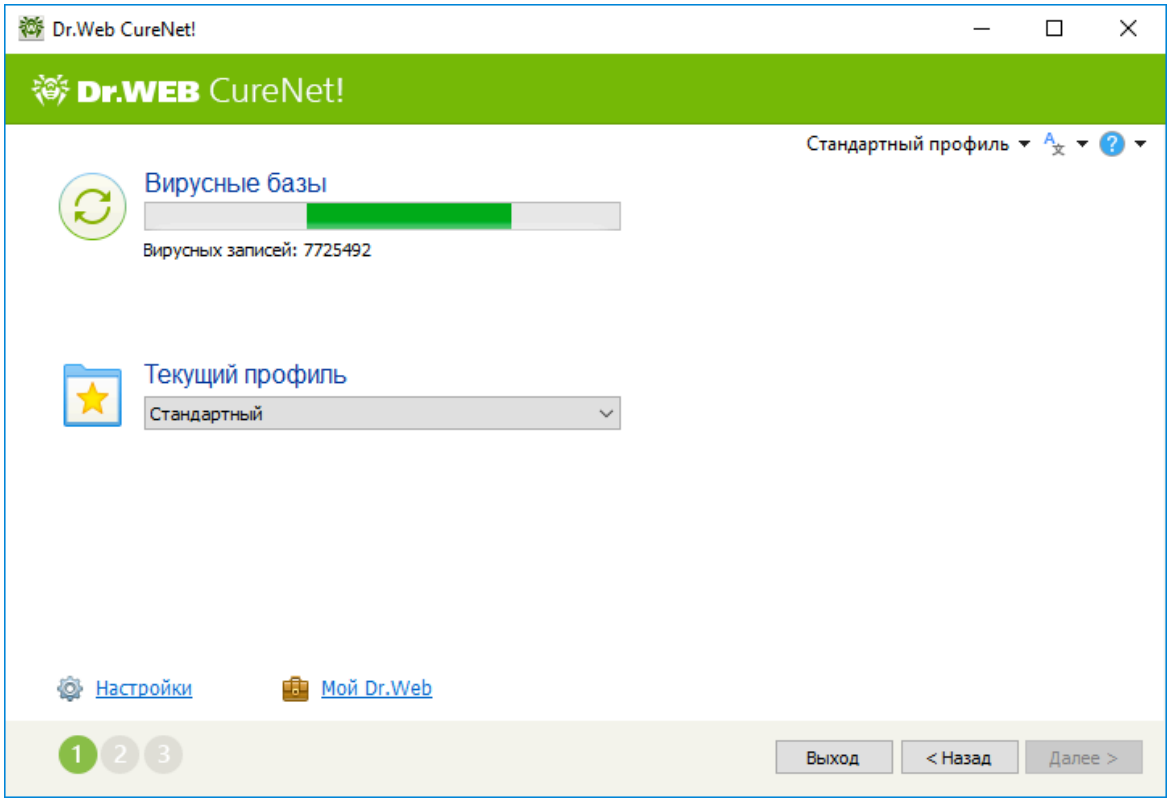
Кроме этого, нажав **О программе** на этой же странице, вы также можете просмотреть информацию о вашей лицензии.



Для продолжения нажмите кнопку **Далее**.

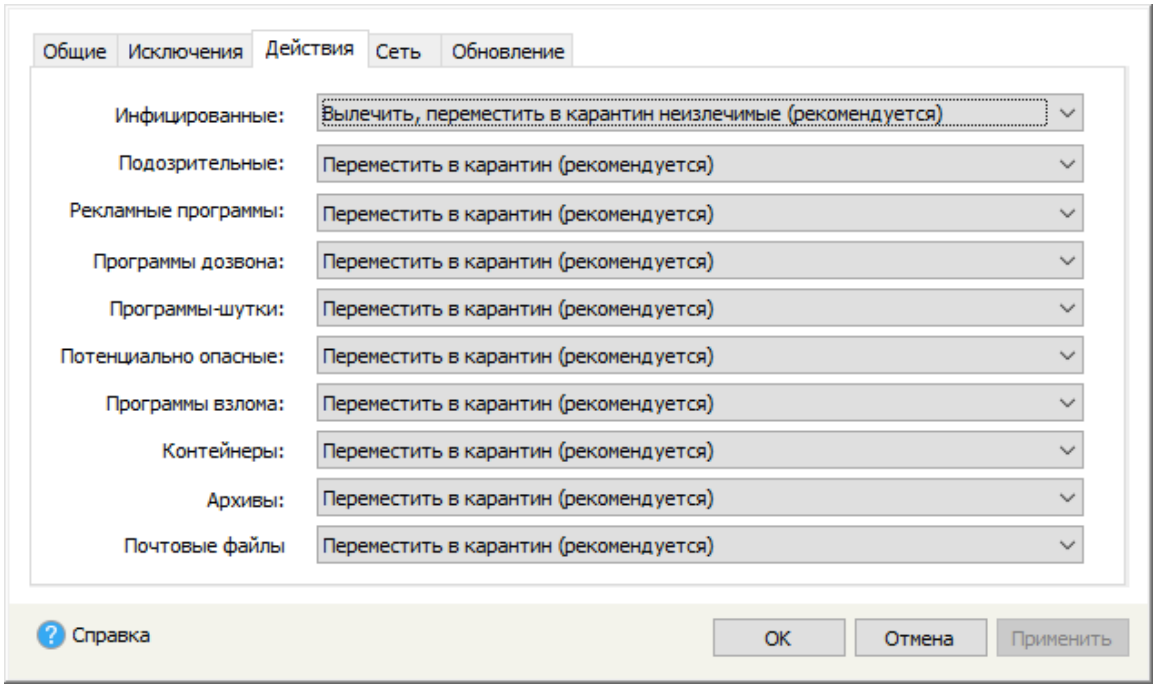


Для обновления антивирусных баз нажмите кнопку **Обновить**.



Внимание! Успешность поиска и удаления вирусов во многом зависит от актуальности антивирусных баз, в связи с чем рекомендуется проводить их обновление при каждом запуске.

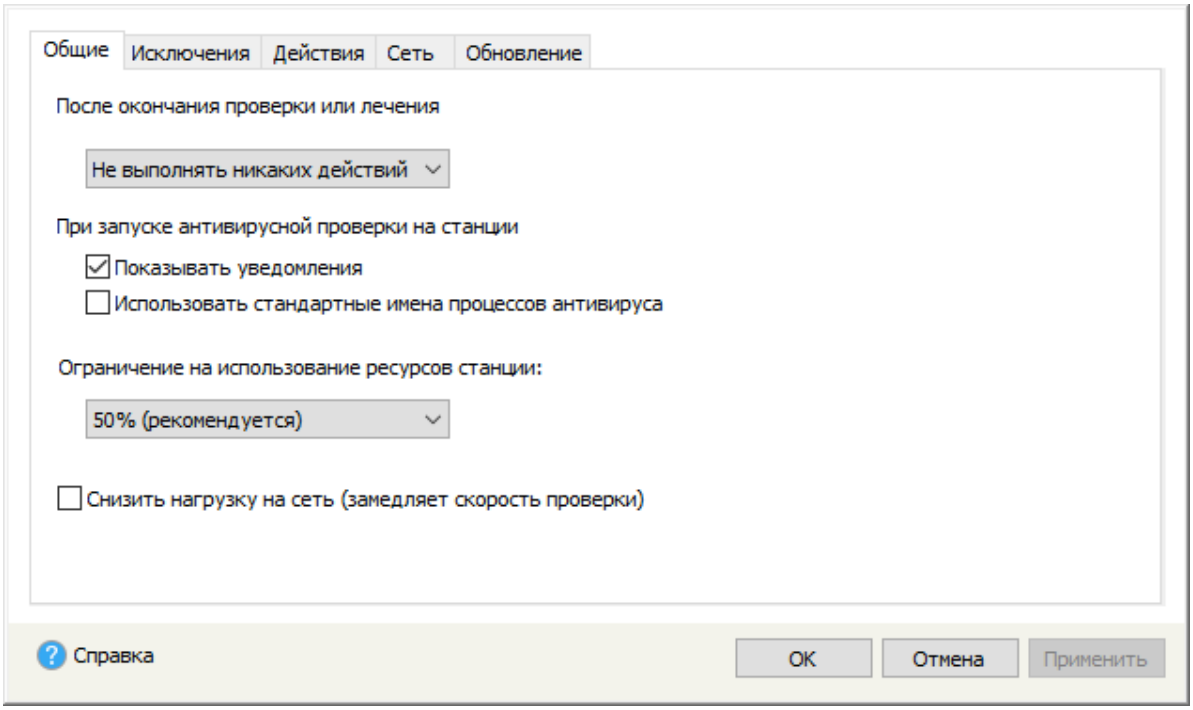
В том случае, если вы хотите изменить настройки по умолчанию, нажмите на **Настройки**.



На закладке **Действия** вы можете выбрать действия, которые будут применяться к вредоносным объектам различного типа. По умолчанию для большинства типов объектов стоит действие **Переместить**.

Необходимо отметить, что для различных объектов список возможных действий является различным. Так, если для инфицированных файлов доступны действия **Вылечить**, **Удалить**, **Переименовать** и **Переместить**, то для неизлечимых пункт **Вылечить** недоступен.

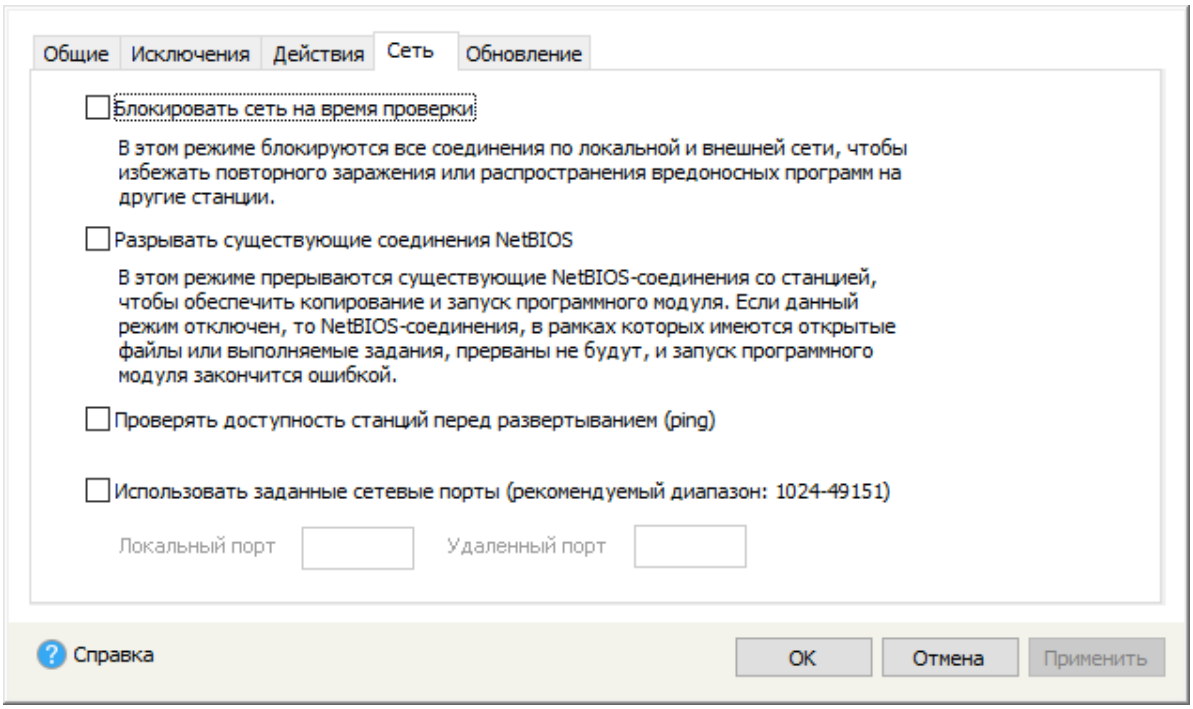
Внимание! Лечение многих вирусов требует перезагрузки, однако пункт **Перезагрузить станцию (закладка Общие)** по умолчанию не отмечен, так как это может нарушить нормальную работу пользователей. В связи с этим рекомендуется при обнаружении вирусов в локальной сети произвести ее полную проверку, уведомив об этом пользователей.



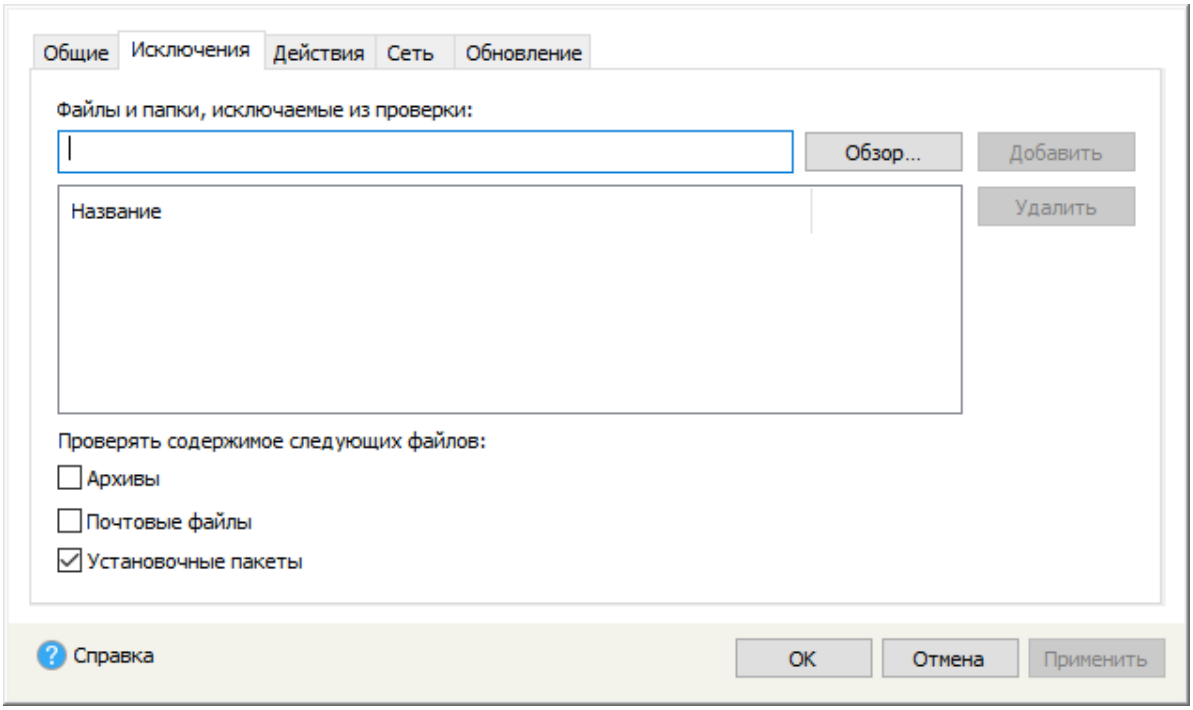
По умолчанию при копировании на проверяемую станцию файлов Dr.Web для них генерируются случайные имена. Если на станции установлен антивирус с брандмауэром, то

администратору может понадобиться при каждой проверке задавать для него исключения. В таком случае рекомендуется включить режим **Использовать стандартные имена процессов антивируса**, чтобы файлы Dr.Web копировались на станции под своими именами. При этом администратору понадобится прописать исключение брандмауэра на проверяемой станции только один раз.

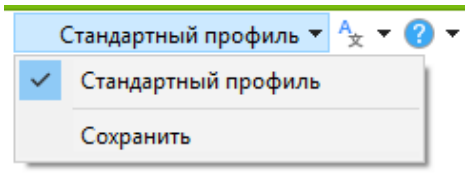
Параметры проверки выбираются на закладке **Сеть**.



На закладке **Исключения** выберите файлы и папки, исключаемые из проверки, а также укажите необходимость проверки упакованных и составных объектов.

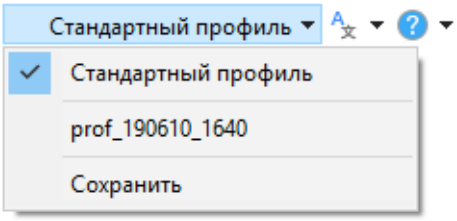


Для сохранения сделанных настроек выберите **Стандартный профиль** и в появившемся меню выберите **Сохранить**.



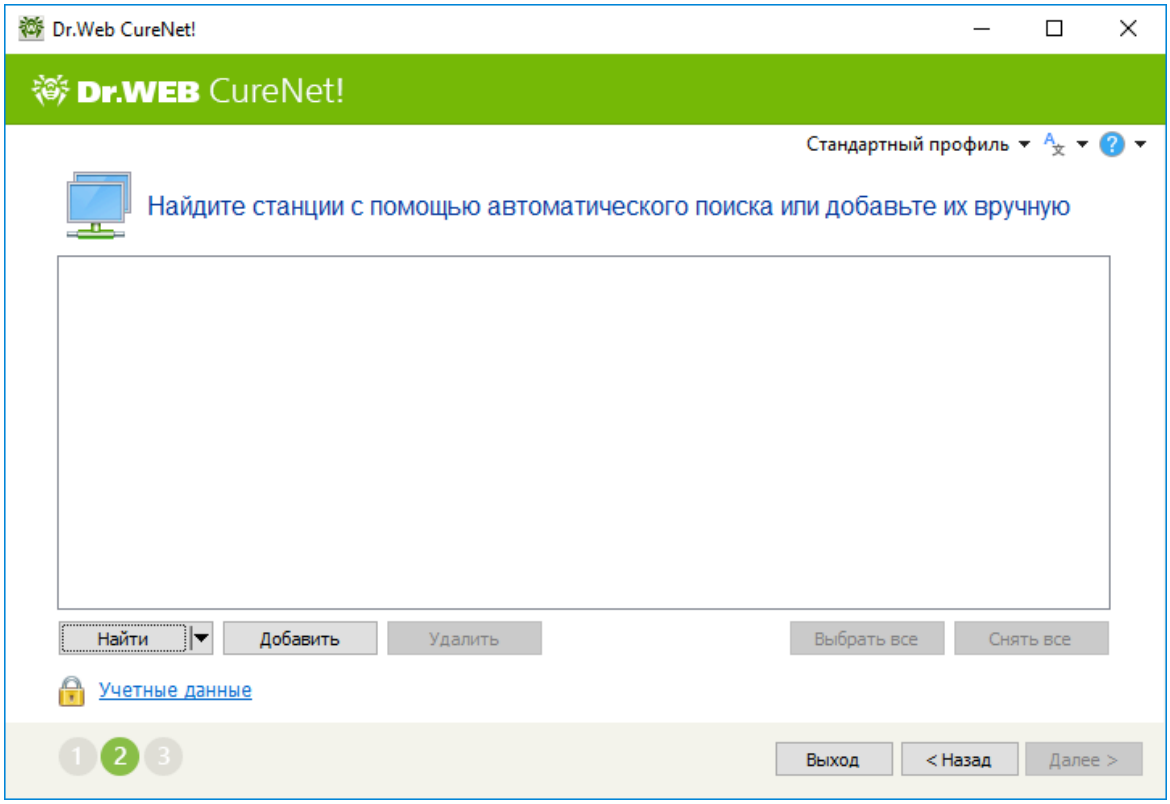
Внимание! Рекомендуется использовать настройки по умолчанию, так как все продукты компании «Доктор Веб» поставляются с установками, оптимизированными для комфортной работы.

В том случае, если у вас уже имеются сохраненные профили, нажмите на **Стандартный профиль** и выберите необходимый вам профиль.

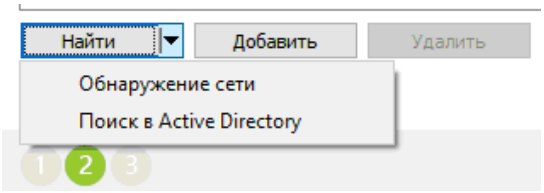


Для продолжения нажмите кнопку **Далее**.

5. В открывшемся окне создайте список станций сети, на которых будет проводиться антивирусная проверка.

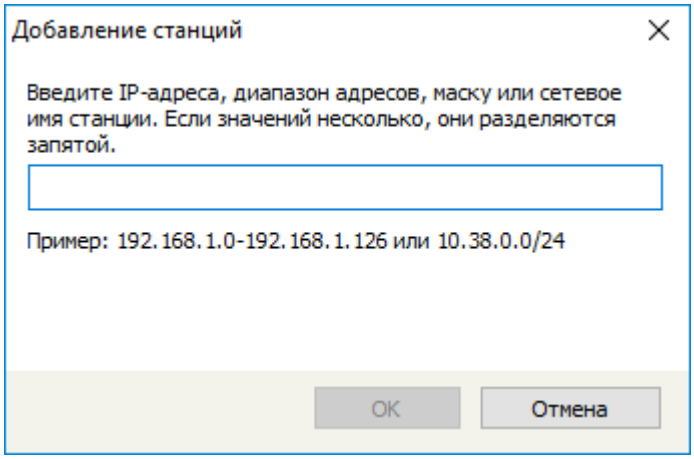


Для поиска компьютеров в сети нажмите **Найти**.



При выборе опции **Обнаружение сети** поиск всех станций может занять длительное время. В любой момент вы можете нажать кнопку **Прервать поиск**. Все станции, обнаруженные на этот момент, будут добавлены в список. Если в процессе поиска станция не была найдена, добавьте ее вручную.

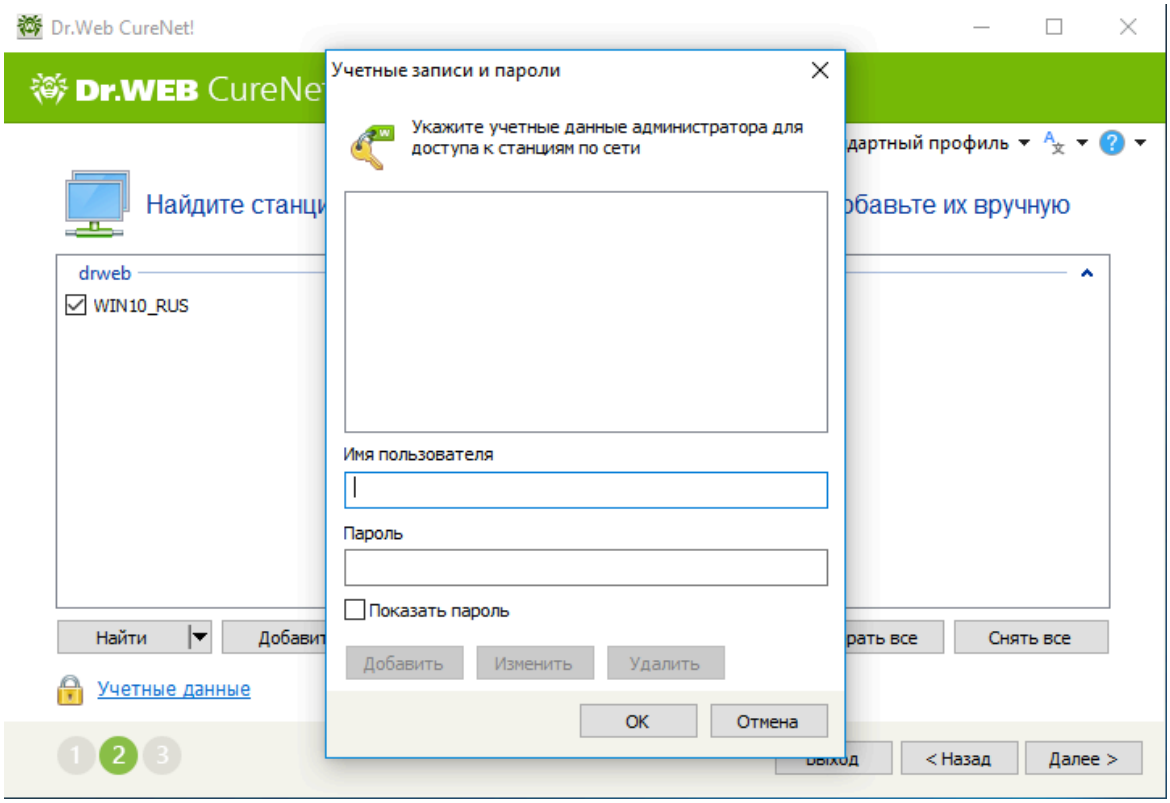
В том случае, если вы хотите сформировать список вручную, вы можете нажать кнопку **Добавить** и в открывшемся окне ввести адрес отдельного компьютера или диапазон проверяемой сети.



Выберите необходимые станции из списка, установив флажок рядом с ее именем или IP-адресом в списке или нажав кнопку **Выбрать все**. Станции, добавленные в список вручную, автоматически выбираются для дальнейшей работы с ними.

В том случае, если проверяемая вами сети не имеет доменной структуры, нажмите **Учетные данные** и в открывшемся окне введите пароли доступа к проверяемым компьютерам.

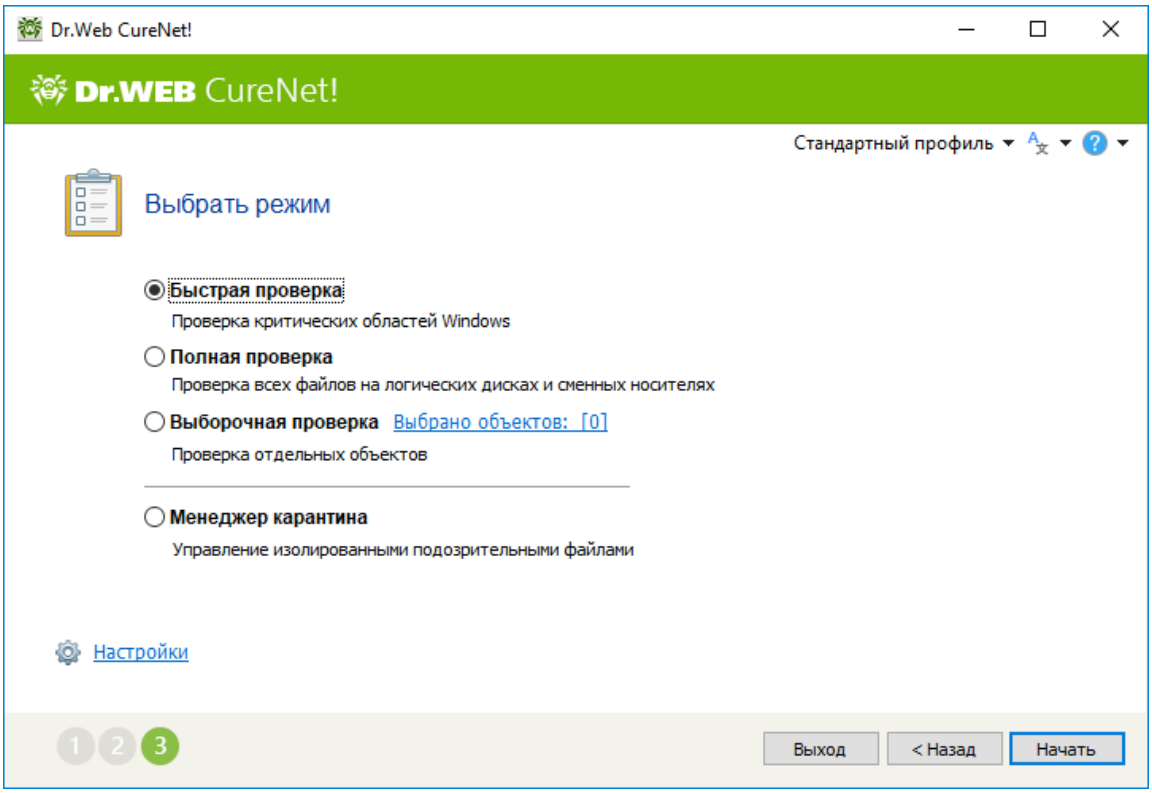
После завершения выбора сформируйте список учетных записей, под которыми Dr.Web будет подключаться к указанным станциям. По умолчанию подключение происходит с правами учетной записи, под которой запущен Мастер. Если подключение под этой учетной записью невозможно, то используются записи из списка.



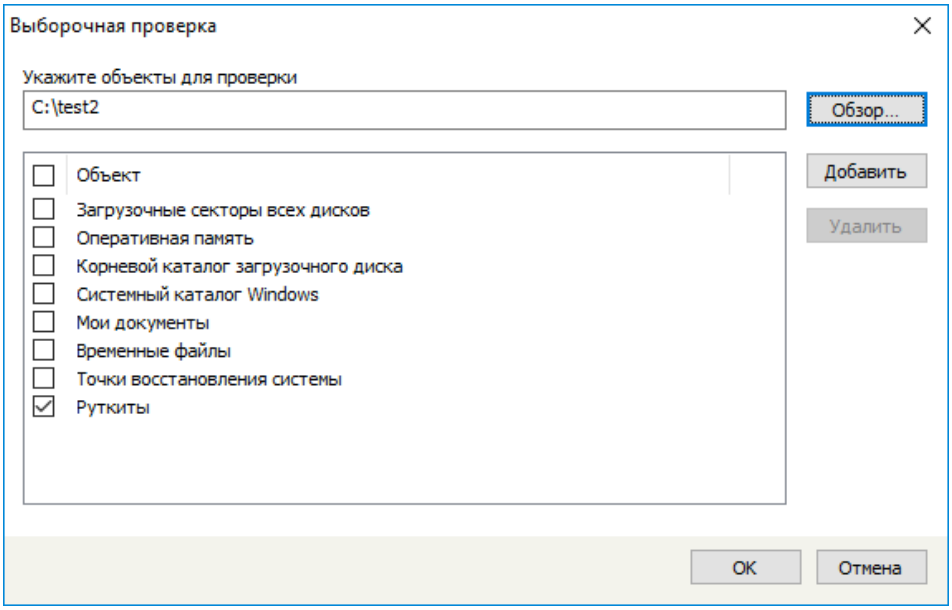
Для продолжения нажмите кнопку **Далее**.

6. В открывшемся окне выберите тип проверки — **Полная, Быстрая** или **Выборочная**.

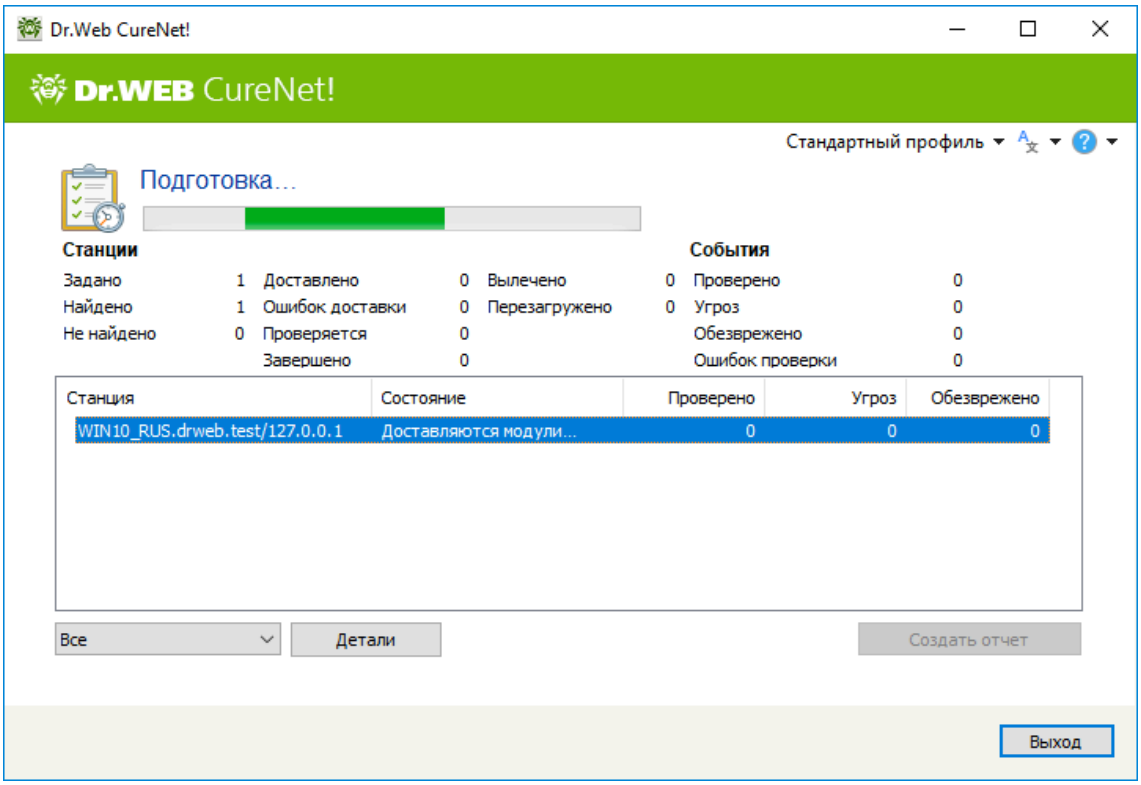
Внимание! В ходе быстрой проверки проверяются только системные области и запущенные процессы, в связи с чем такая проверка не гарантирует полной очистки вашего компьютера от вирусов. В частности, потому, что работающие вирусы могут заражать уже проверенные («чистые») файлы.



Если вы выбрали выборочную проверку, укажите список объектов для проверки.



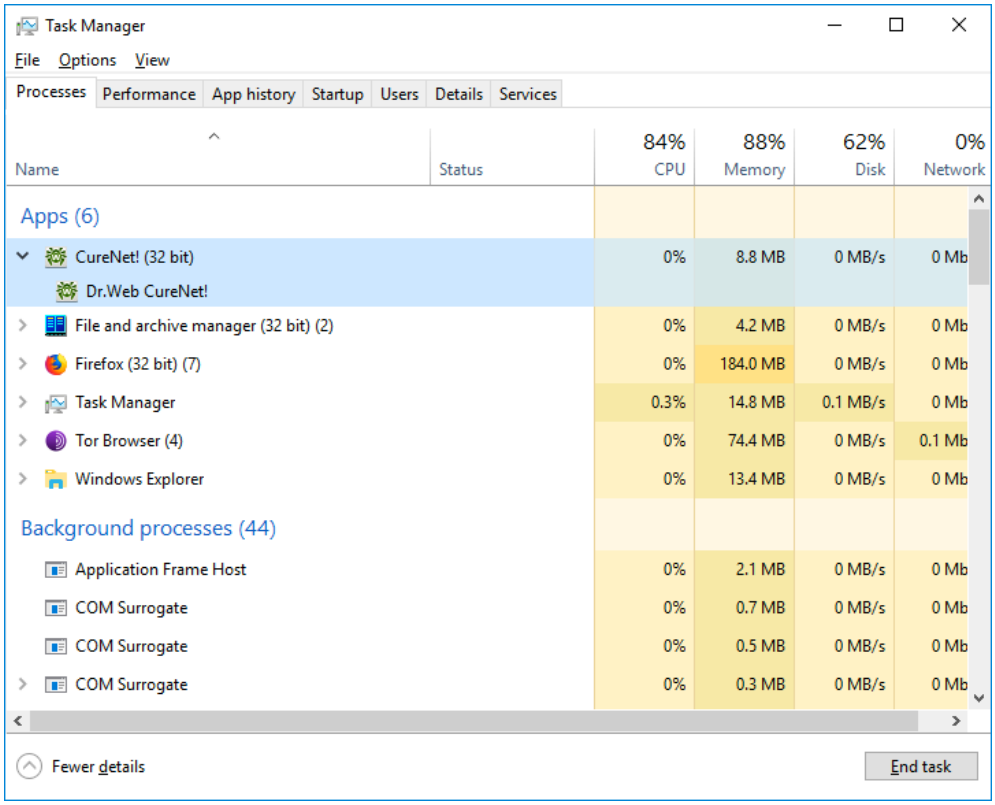
Для продолжения нажмите кнопку **Начать**.



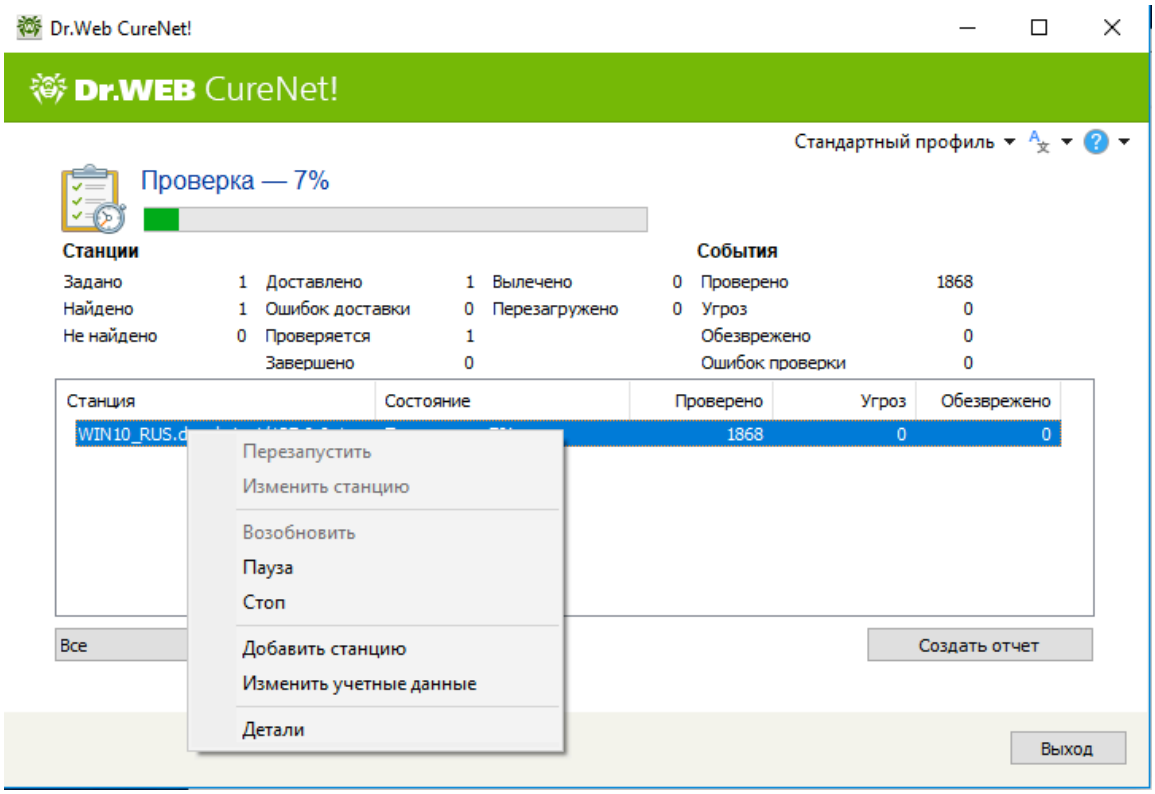
На этой странице отображаются ход и результаты сканирования на удаленных компьютерах сети. Предоставляемая статистика не зависит от качества соединения между компьютерами. Даже если соединение будет прервано, Dr.Web CureNet! обновит статистику при его восстановлении.

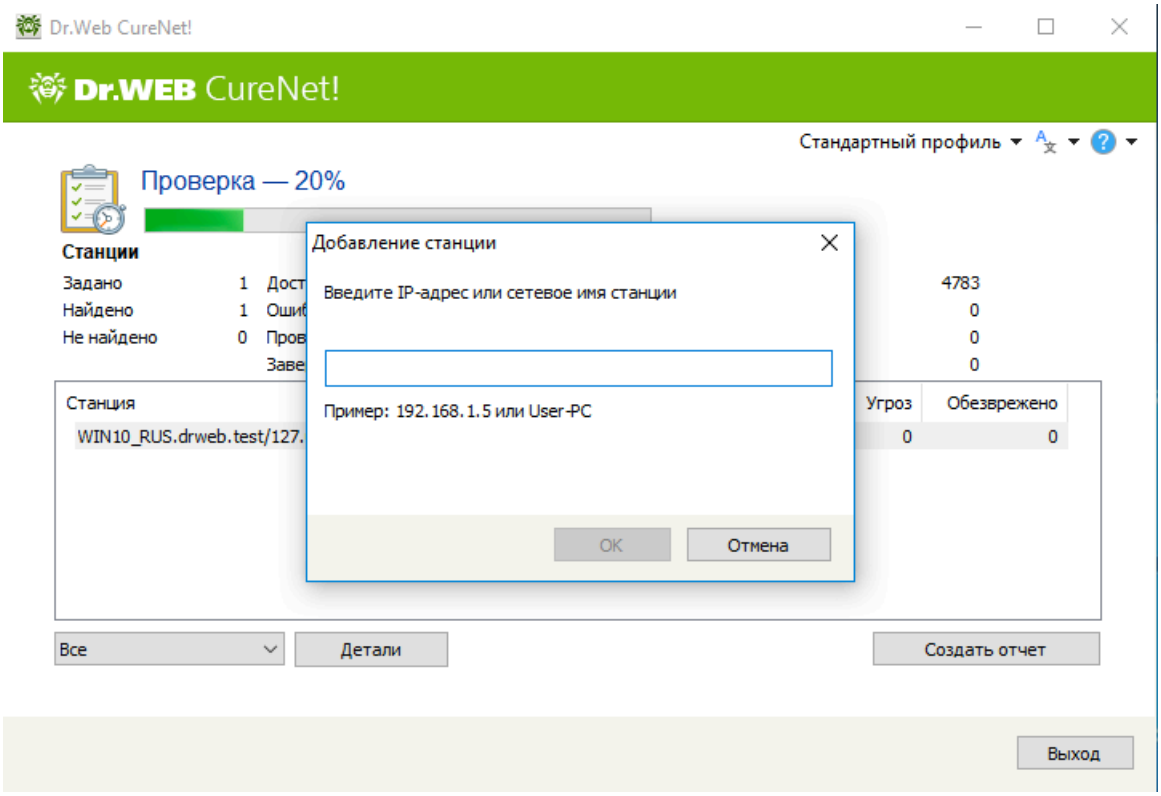
Внимание! Не рекомендуется прерывать проверку досрочно.

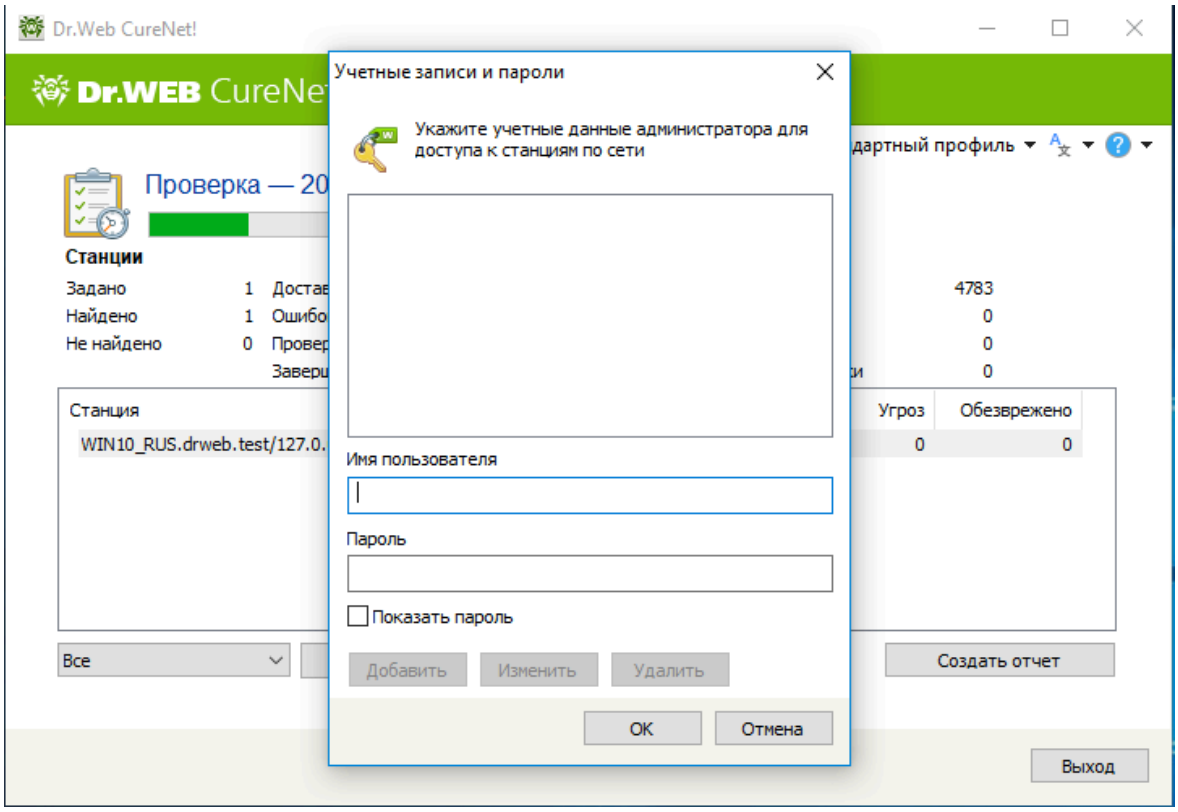
Запущенные процессы проверки используют механизмы самозащиты от действий вредоносных программ.



Использование контекстного меню позволяет остановить или продолжить проверку, на лету добавить станцию или изменить учетные данные.





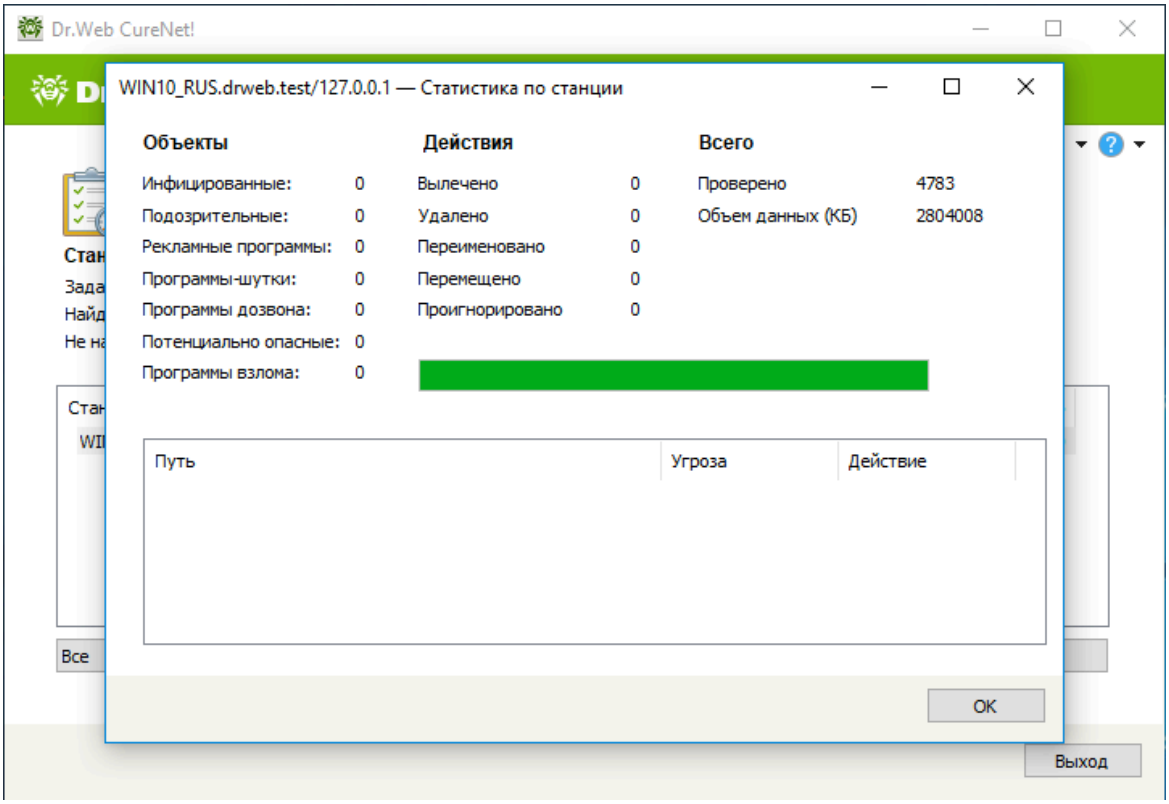


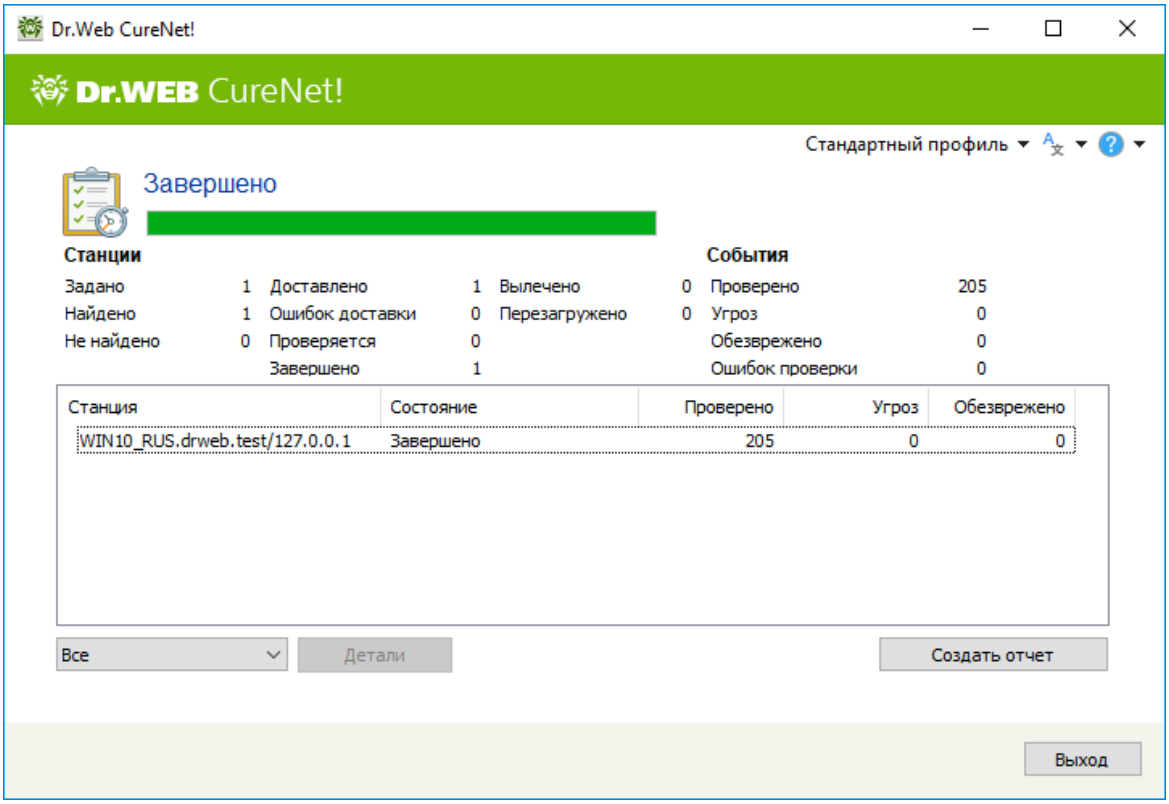
Внимание!

- Действия над некоторыми зараженными или подозрительными объектами (например, ключами реестра, файлами, используемыми другими приложениями Windows) не могут быть выполнены немедленно. При обнаружении такие файлы помечаются как подлежащие обработке (в зависимости от заданного действия) после перезагрузки станции. Для корректной обработки подобных объектов вы можете разрешить перезагружать операционные системы проверенных станций при необходимости или выключать их автоматически после окончания сканирования. При этом пользователю станции будет выводиться соответствующее предупреждение и выделяться время на завершение текущей работы и сохранение информации.
- При обнаружении вирусов в главной загрузочной записи операционной системы (MBR) Сканер Dr.Web применяет обязательную перезагрузку станции непосредственно после обнаружения вируса и восстановления записи (так называемая «жесткая» перезагрузка). Перезагрузка выполняется вне зависимости от того, установлен флажок **Перезагрузить станцию** или нет.

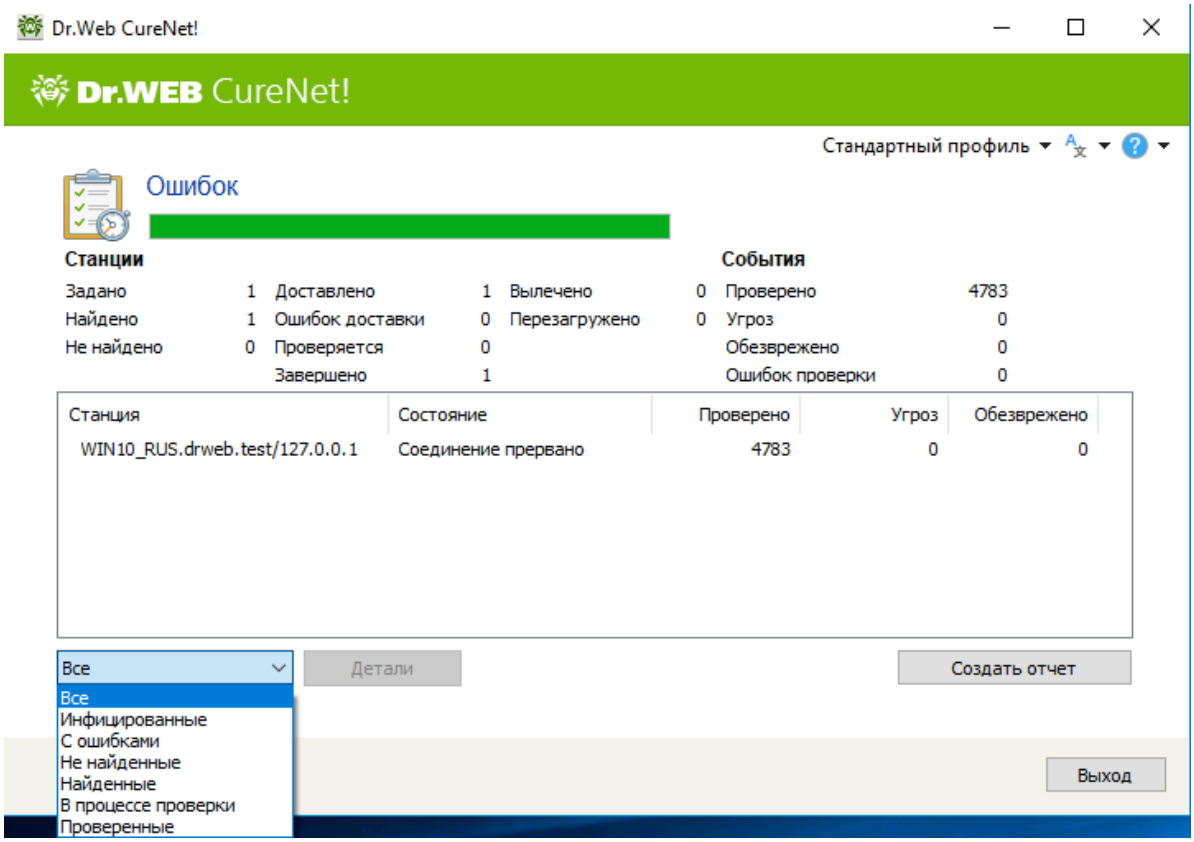
Процесс проверки станций не зависит от того, запущен или нет Мастер. Для выхода из Мастера нажмите кнопку **Выход**. При этом процесс проверки не прекращается, но статистика работы становится недоступной.

Нажав на кнопку **Детали**, вы получите отображение подробной статистики.

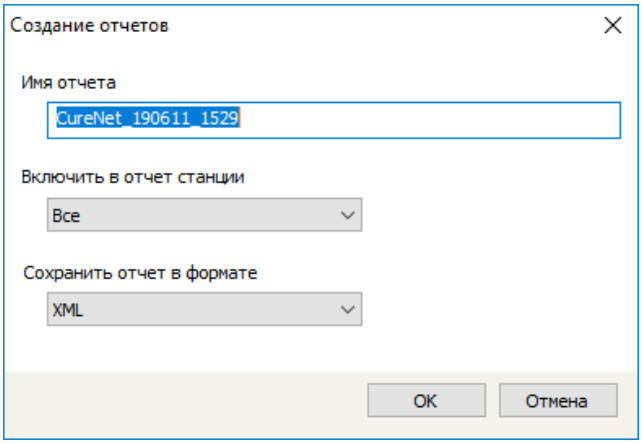


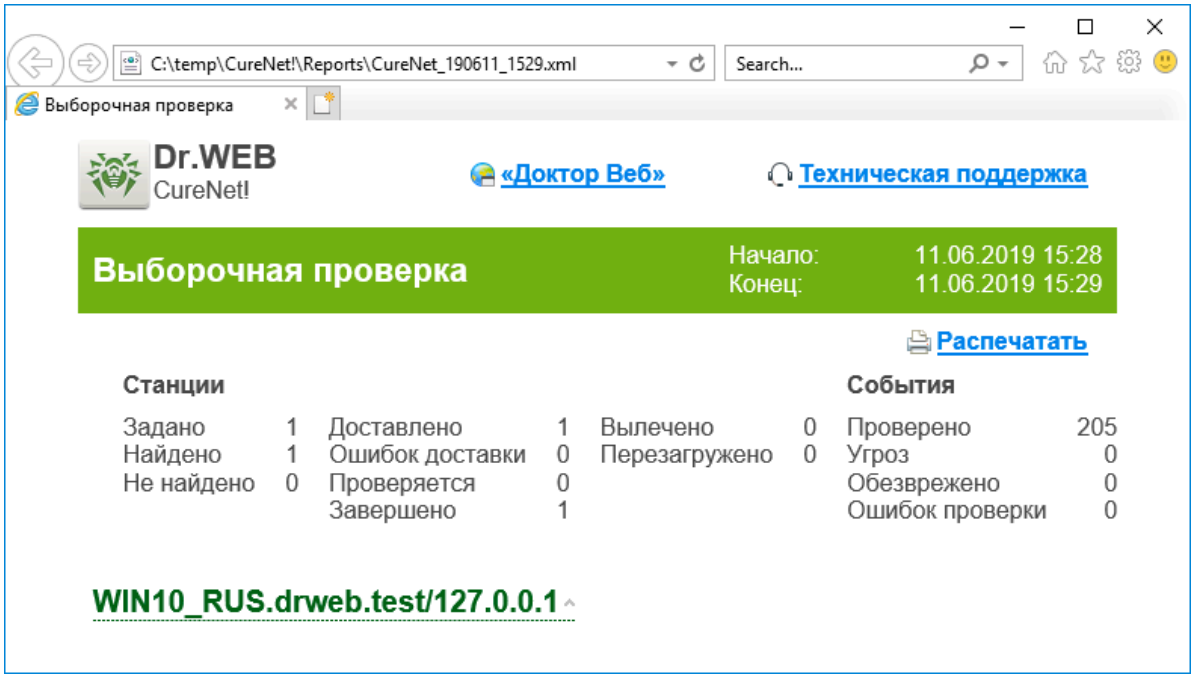


Нажав на выпадающее меню, вы можете выбрать режим отображения.



Вы можете сформировать отчет о проверке сети, нажав на кнопку **Создать отчет**.





Для завершения работы нажмите кнопку **Выход**.

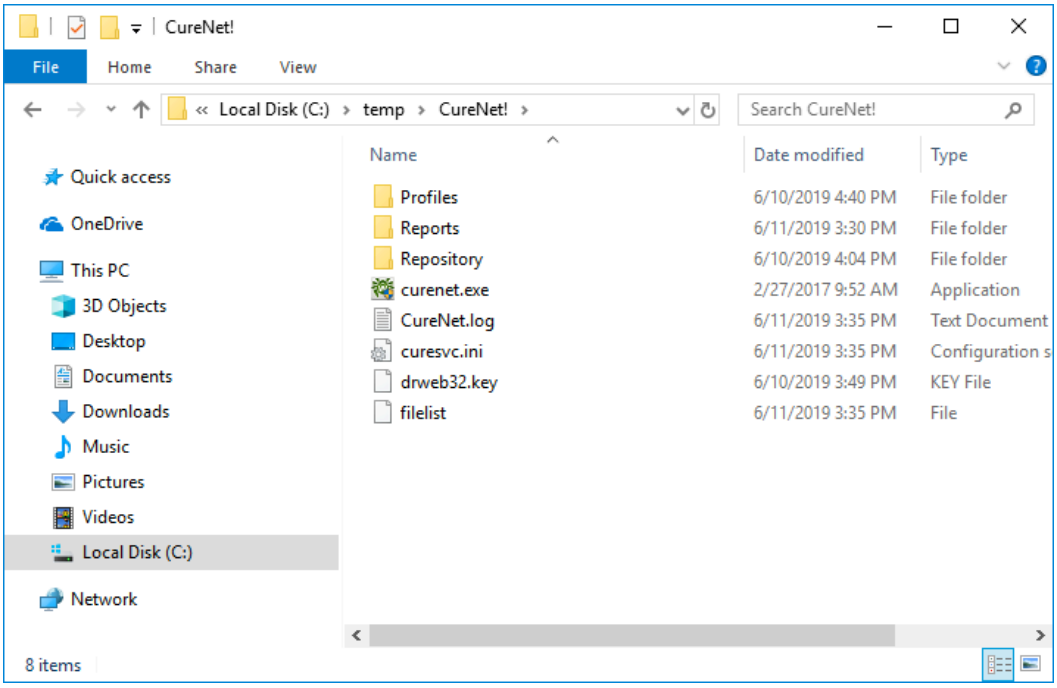
Подробные инструкции по использованию продукта, настройкам сканирования, созданию и сохранению профилей доступны в Руководстве администратора Dr.Web CureNet!.

Использование Dr.Web CureNet!

Рекомендуется проводить антивирусную проверку системы регулярно. В частности, в связи с тем, что проверенные файловым монитором и записанные на диск файлы могут содержать вирусы, неизвестные на момент проверки.

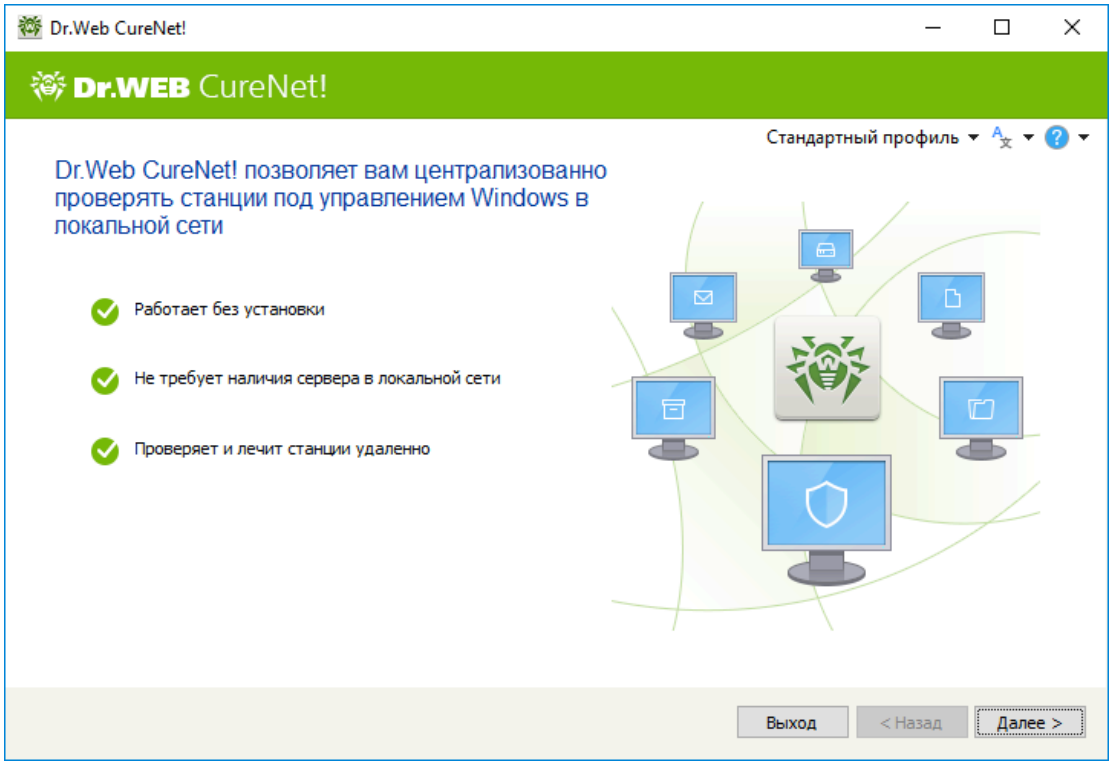
Для проведения проверки:

1. Откройте папку, куда в ходе первого запуска были сохранены файлы **Dr.Web CureNet!** (по умолчанию это папка **CureNet** в каталоге, где вы запустили установочный файл утилиты, или **Рабочий стол**, если вы сохранили установочный файл на него), и запустите файл **CureNet**.



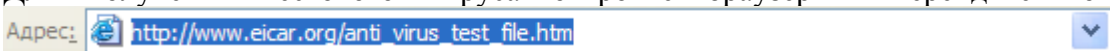
Если вы используете систему UAC, то далее вам нужно будет подтвердить запуск программы, нажав на **Да**.

Дальнейшая процедура работы с продуктом не отличается от описанной выше.

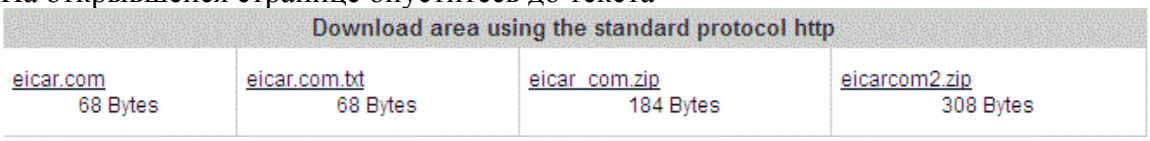


Проверка работоспособности продукта

1. Для получения тестового вируса откройте браузер и перейдите по адресу



2. На открывшейся странице опуститесь до текста



и выберите для скачивания любой из предложенных вариантов, например первый — eicar.com.

3. Сохраните полученный файл на рабочем столе проверяемого компьютера.

   Внимание! Если вы используете Dr.Web CureNet! в дополнение к антивирусным продуктам других производителей, отключите их перед сохранением тестового файла.

4. Запустите Dr.Web CureNet! и проведите антивирусную проверку.

Анализ вредоносных файлов специалистами антивирусной лаборатории «Доктор Веб»

Ни один автоматизированный сервис никогда не заменит опыт и знания вирусного аналитика. В случае если вердикт Dr.Web vxCube о проанализированном файле будет не однозначно вредоносный, но у вас останутся сомнения в этом решении, предлагаем воспользоваться услугами специалистов антивирусной лаборатории «Доктор Веб» с многолетним опытом вирусного анализа.

Услуги включают анализ вредоносных файлов любой сложности, по результатам которого выдается отчет, содержащий:

- описание алгоритма работы вредоносного ПО и его модулей;
- категоризацию объектов: однозначно вредоносный, потенциально вредоносный (подозрительный), др.;
- анализ сетевого протокола и выявление командных серверов;
- влияние на зараженную систему и рекомендации к устранению заражения.

Заявки на антивирусные исследования принимаются по адресу: https://support.drweb.ru.

Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

Если ваша компания пострадала от действия вредоносного ПО и требуется квалифицированная экспертиза произошедшего вирусных аналитиков, воспользуйтесь услугами специального подразделения компании «Доктор Веб».

Экспертиза ВКИ включает:

- Предварительную оценку инцидента, объема экспертизы и мер, необходимых для устранения последствий произошедшего.
- Экспертные исследования компьютерных и других артефактов (накопителей на жестких магнитных дисках, текстовых, звуковых, фото-, видеоматериалов), предположительно имеющих отношение к ВКИ.
- Не имеет аналогов! Психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика (комплексное определение рисков), а также фактов бездействия или халатного отношения к служебным обязанностям.
- Рекомендации по вопросам построения антивирусной системы защиты с целью недопущения ВКИ или сокращения их количества в будущем.

Полезные ссылки

Об экспертизе ВКИ: https://antifraud.drweb.ru/expertise

Заявки на экспертизу: https://support.drweb.ru/expertise

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу

продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей — по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТ ЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  - отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	Сертификаты Минобороны России	Сертификаты ФСБ России	Все сертификаты и товарные знаки

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Тел.: +7 495 789–45–87 (многоканальный)

Факс: +7 495 789–45–97

антивирус.рф | www.drweb.ru