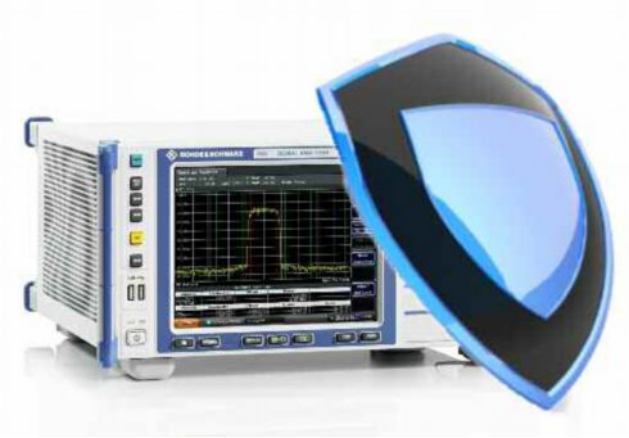
Защита от вредоносного программного обеспечения

Техническое описание



Компания Rohde & Schwarz осознает потенциальный риск заражения компьютерными вирусами измерительного оборудования на базе ОС Windows® при его подсоединении к другим компьютерам через локальные сети или при использовании съемных устройств хранения данных.

В настоящем документе описаны меры по минимизации угроз со стороны вредоносного ПО и рассмотрены способы уменьшения возможных рисков без ухудшения рабочих характеристик измерительных приборов.

В документе рассмотрено использование антивирусного ПО и приведены его рекомендуемые настройки. Здесь также изложены рекомендации по поддержанию ОС Windows® XP в актуальном состоянии с помощью регулярных обновлений системы.

ROHDE&SCHWARZ

Защита от вредоносного ПО
Техническое описание
Jochen Wolle
06.2010-1EF73_0e

Содержание

1 Приборы на базе ОС Windows®

1.1 Введение

Компания Rohde & Schwarz стремится к тому, чтобы все поставляемые продукты компании были гарантированно свободны от вирусов. Приборы, работающие под управлением операционной системы Windows, должны быть защищены от вредоносного ПО так же, как и любой другой персональный компьютер. Пользователям строго рекомендуется принимать следующие меры для защиты своих приборов: использовать антивирусное ПО, устанавливать исправления и обновления ОС на регулярной основе. Также настоятельно рекомендуется работать в тесном сотрудничестве с отделом информационных технологий или системным администратором, чтобы при подсоединении приборов к локальной сети вашей компании были соблюдены все ее требования по информационной безопасности.

1.2 Программа контроля за распространением компьютерных вирусов

Компания Rohde & Schwarz осознает потенциальный риск заражения компьютерными вирусами измерительного оборудования на базе ОС Windows при его подсоединении к локальным сетям (LAN).

Внутри компании Rohde & Schwarz были введены правила, направленные на принятие всех обоснованных мер предосторожности для предотвращения распространения вирусов из приборов на компьютеры и сети наших клиентов:

- Все используемые в компании Rohde & Schwarz компьютеры, которые могут быть подсоединены к предназначенным для наших клиентов приборам, оснащены централизованно управляемым брандмауэром (межсетевым экраном) и антивирусным программным обеспечением с актуальным набором описаний вирусов. Во избежание распространения компьютерных вирусов производится регулярное сканирование компьютеров и съемных устройств хранения данных.
- Введены жесткие правила контроля за распространением компьютерных вирусов в условиях производства, ремонта, обслуживания, продажи, распространения и демонстрации продукции компании. В зависимости от конфигурации прибора они включают в себя использование изолированных локальных сетей, сканирование приборов и съемных носителей и/или полное восстановление информации на жестких дисках.
- Для всех сотрудников компании Rohde & Schwarz, которые соприкасаются с приборами клиентов, установлены процедуры по усилению мер антивирусной безопасности. Они затрагивают весь персонал, занятый в производстве, ремонте, обслуживании, продаже и распространении продукции компании.

1.3 Аспекты профилактического обслуживания

Описанные выше меры позволяют гарантировать, что любой прибор компании Rohde & Schwarz не будет содержать вирусов на момент поставки его заказчику. С момента поставки за информационную безопасность прибора отвечает сам пользователь.

Перед подсоединением прибора к локальной сети вашей компании следует проконсультироваться с отделом информационных технологий или системным администратором о существующих требованиях по информационной безопасности. Помните, что в сети прибор виден как стандартный компьютер. Выполняйте требования вашей компании по компьютерной безопасности и антивирусной защите.

Кроме того, важно регулярно выполнять обновления операционной системы и антивирусных баз. Компания Rohde & Schwarz, в дополнение к сканированию прибора на наличие вредоносного ПО, рекомендует выполнять проверку обновлений операционной системы и антивирусных баз не менее одного раза в неделю. Обязательно обновляйте ОС и антивирусные базы по указанию отдела информационных технологий или системного администратора. Чтобы обеспечить защиту операционной системы прибора, следует предпринять следующие меры:

- Использовать на приборе интернет-брандмауэр.
- Регулярно сканировать все съемные устройства хранения данных (например, USB-накопители), которые используются при работе с прибором, а также отключить функцию автоматического запуска/воспроизведения *Autorun* / *Autoplay* для предотвращения непреднамеренного выполнения вредоносного кода с этих устройств.
- Установить на прибор последние исправления и обновления ОС Windows®.
- Регулярно сканировать прибор с помощью антивирусного ПО и обновлять файлы антивирусных баз. Настоятельно НЕ рекомендуется запускать антивирусное ПО в фоновом режиме (режим резидентного сканирования), так как это оказывает значительное влияние на производительность прибора.

1.4 Учетная запись пользователя / администратора

Для работы с ОС Windows необходимо, чтобы пользователи прошли процедуру идентификации путем ввода имени и пароля в окне входа в систему. Как правило, в приборах компании R&S по умолчанию настроена функция автоматического входа в систему, т.е. вход в систему выполняется автоматически при загрузке прибора. При этом пользователь получает права администратора с неограниченным доступом, что позволяет ему установить принтер или задать сетевые настройки прибора.

Для многих приборов может быть установлено два типа учетных записей пользователя: это либо запись администратора с неограниченным доступом к ОС прибора, либо запись обычного пользователя с ограниченным доступом. Настройками учетных записей можно управлять в окне **Windows Start ⇨ Control Panel ⇨ User Accounts**. Более подробную информацию об изменении или добавлении новых пользователей и об отключении функции автоматического входа в систему см. в руководстве по эксплуатации прибора.

Примечание – Для изменения настроек брандмауэра, установки и конфигурирования антивирусного ПО, а также обновления ОС Windows необходимы неограниченные права администратора.

2 Настройки брандмауэра

В ОС Windows XP SP2 и более поздних версиях для защиты компьютера или прибора от атак из внешней сети может быть применен брандмауэр (межсетевой экран). Приборы компании R&S поставляются с уже включенным и предварительно настроенным брандмауэром Windows (Windows firewall). Действующий на приборе брандмауэр будет полезен даже в случае, если прибор включен в защищенную сеть вашей компании. При наличии в сегодняшнем интернете огромного числа червей, вирусов и прочего вредоносного ПО что-нибудь из вышеперечисленного неминуемо сможет проникнуть через корпоративный брандмауэр. Установленный на приборе брандмауэр не только способствует защите от угроз внутри корпоративного периметра, но и препятствует распространению множества вирусов и червей.

Если к прибору предъявляются дополнительные требования по информационной защите и безопасности, следует связаться с вашим отделом информационных технологий или системным администратором, чтобы согласовать их с политикой информационной безопасности вашей компании.

2.1 Конфигурация портов брандмауэра

Приборы компании R&S предварительно настроены таким образом, что доступными являются все порты и соединения для дистанционного управления. Подробности см. в следующей таблице:

Порт	*Служба*	*Описание*
21 tcp	FTP	Веб-сервер прибора (порт FTP)
80 tcp (HTTP)	Web server	Веб-сервер прибора (LXI)
111 tcp, 111 udp	Portmapper	Служба назначения портов для VXI-11 / LXI
161 udp 162 udp 705 tcp (AgentX)	SNMP	Стандартные порты для SNMP-агента
319 tcp udp 320 tcp udp	1588 PTP	LXI Класс B/A – IEEE1588 PTP (протокол точного времени)
2525 tcp	RSIB	Соединение гнезда R&S SCPI
4880 tcp	HiSLIP	Протокол высокоскоростного сетевого интерфейса
5025 (данные) 5125 (прекращение)	TCP Socket	Соединение гнезда ‘Raw SCPI’
5044 tcp udp	LXI Class B	Сетевые сообщения и события LXI Групповой адрес для udp: 224.0.23.159
5800 tcp 5900 tcp	VNC	Программная передняя панель прибора, реализуемая через веб-сервер (интерфейс браузера)
13217 tcp udp	RS Installer	Служба распространения ПО от R&S
14142 - 16383 tcp udp (динамическое назначение)	ONC-RPC	Протокол Sun ONC-RPC (VXI-11)

2.2 Изменение настроек брандмауэра

Компания Rohde & Schwarz настоятельно рекомендует использовать на приборе брандмауэр (межсетевой экран).

Следует иметь в виду, что для изменения настроек брандмауэра необходимо обладать правами администратора. Управление настройками брандмауэра производится в окне **Windows Start ⇨ Control Panel ⇨ Windows Firewall**:

Проблемы, которые связаны со стандартной конфигурацией брандмауэра, могут проявляться двояким образом:

- Клиентские программы могут не получить данные из прибора.
- Серверные программы, которые выполняются на приборе, могут не отвечать на клиентские запросы.

Если программа блокируется брандмауэром, пользователь может получить следующее оповещение системы безопасности Windows (Windows Security Alert):

Для разблокировки такой программы следует нажать кнопку **Unblock** в диалоговом окне **Windows Security Alert**. Подробное описание по установке и конфигурированию брандмауэра можно найти по адресу:

http://support.microsoft.com/kb/875357/en-us

3 Устройства USB

В настоящее время в работе повсеместно применяются флэш-накопители USB (флэшки) и переносные жесткие диски, поскольку они обладают значительной емкостью и ими удобно пользоваться для сохранения настроек прибора, результатов измерений, печатных копий и т.п. Однако их использование порождает новые проблемы: огромное число вирусов, программ-троянов и прочего вредоносного ПО заражают компьютеры через USB-устройства хранения данных. Как только зараженный флэш-накопитель USB будет подключен к прибору, содержащееся на нем вредоносное ПО может распространиться по всей сети.

3.1 Отключение функции автозапуска USB-устройств

Обычно вирусы, которые распространяются через флэш-накопители USB, используют функцию «автозапуска» Windows, так как она не требует подтверждения на запуск и незаметно выполняется в фоновом режиме. В приборах компании R&S функция автозапуска/автовоспроизведения отключена. Тем самым блокируется автоматическое выполнение любого вредоносного ПО непосредственно с флэш-накопителя USB.

Управление или изменение данной настройки осуществляется с помощью редактора групповых политик Group Policy Editor.

Если прибор используется в корпоративной сети и является членом сетевого домена, то групповые политики могут конфигурироваться централизованно – отделом информационных технологий или системным администратором.

- Перейти в окно **Windows Start ⇨ Run** и ввести команду **gpedit.msc** для того, чтобы открыть редактор групповых политик.
- Перейти в раздел **Computer Configuration ⇨ Administrative Templates ⇨ System**, пролистать список и дважды щелкнуть на записи **Turn off Autoplay** для того, чтобы открыть диалоговое окно настроек:

- Выбрать позицию кнопки-переключателя **Enabled**, затем из выпадающего списка «**Turn off Autoplay on**» выбрать значение **All drives** для того, чтобы запретить автоматическое выполнение любых программ с любых USB-накопителей или съемных носителей.

- **Примечание –** Если в списке шаблонов отсутствует **System**, необходимо добавить шаблон настроек. Для этого правой кнопкой мыши щелкнуть на пункте **Administrative Templates** и выбрать команду **Add/Remove Templates…**. В открывшемся диалоговом окне нажать **Add** и выбрать шаблон «system.adm». Нажать **Open**, затем **Close**, чтобы вернуться в главное окно.

Подробные сведения о функции автозапуска можно найти по адресу:
http://support.microsoft.com/kb/967715/en-us

3.2 Сканирование USB-устройств

Компания Rohde & Schwarz рекомендует выполнять сканирование флэш-накопителей USB и переносных жестких дисков с помощью антивирусного ПО на регулярной основе, препятствуя появлению на них вредоносного ПО.

Перед подключением USB-устройств хранения данных к приборам компании R&S следует просканировать их на наличие вредоносного ПО на своем компьютере с помощью своего антивирусного ПО.

4 Антивирусное программное обеспечение

Пользователи должны предпринимать соответствующие меры для защиты измерительных приборов от заражения так же, как на обычных персональных или рабочих компьютерах. Помимо использования строгих правил настройки брандмауэра и регулярного сканирования всех съемных устройств хранения данных, используемых вместе с прибором R&S, рекомендуется также установить на прибор антивирусное программное обеспечение. И хотя компания Rohde & Schwarz **НЕ рекомендует** запускать на Windows-приборах антивирусное ПО в фоновом режиме (режим резидентного сканирования) из-за возможности ухудшения производительности прибора, следует запускать данное ПО, по крайней мере, один раз в неделю в свободное от нагрузки время.

Для имеющегося в настоящее время антивирусного ПО требуется значительный объем системных ресурсов (свободное пространство на жестком диске и объем оперативной памяти). Следовательно, на некоторых приборах из-за ограниченного объема их ресурсов нельзя будет установить или запустить антивирусное ПО. В таких случаях приборы можно сканировать с помощью ПО, запускаемого с флэш-накопителя USB, или подключить их в виде сетевого диска, а затем просканировать с помощью антивирусного ПО с другого компьютера. Подробнее эти возможности будут рассмотрены далее.

Примечание – В следующих разделах подчеркиваются основные рекомендации по настройке антивирусного ПО на примере нескольких широко распространенных программ. Несомненно, что существует множество других подобных программ; программы, описанные в следующих разделах, служат в качестве общих примеров, а рассмотренные принципы настройки могут применяться к другим программам, используемым вашим отделом информационных технологий или системным администратором.

Для установки, настройки и использования антивирусного ПО необходимо обладать правами администратора.

4.1 Программа Norton™ AntiVirus 2010

В данном разделе описана установка, настройка и использование антивирусного ПО Norton AntiVirus 2010 в приборах компании R&S.

4.1.1 Установка программы

Установить на прибор программу Norton AntiVirus 2010 в соответствии с описанием программного руководства. На установочной странице приветствия снять флажок с функции **I want to join the fight...** и запустить установку кнопкой **Agree & Install**:

По окончании установки программа Norton AntiVirus 2010 попытается соединиться с сервером компании Symantec для того, чтобы получить последние описания вирусов и программные обновления (данный процесс называется *LiveUpdate*).

4.1.2 Системные требования

Для установки и работы с ПО Norton AntiVirus 2010 должны выполняться следующие требования:

- 200 Мбайт свободного пространства на жестком диске прибора
- 256 Мбайт оперативной памяти
- ОС Windows XP SP2 и выше

Убедиться, что на вашем приборе компании R&S установлена версия ОС не ниже Windows XP SP2. Способ проверки текущей версии ОС описан в руководстве по эксплуатации прибора. Если прибор работает под управлением ОС более ранней версии, рекомендуется связаться с вашим представительством компании R&S на предмет возможного обновления ОС. Для многих приборов компания R&S предоставляет DVD-диск восстановления с последней версией ОС, предназначенный для полного восстановления данных на жестком диске прибора.

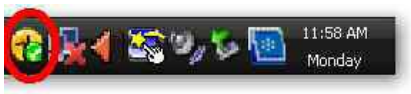
Во время выполнения процедуры обновления *LiveUpdate* или сканирования на вирусы в приборе выполняются два процесса (оба с именем **ccSvcHst.exe)**, которые занимают **до 270 Мбайт** памяти.

Таким образом, компания Rohde & Schwarz рекомендует останавливать встроенное ПО прибора перед запуском процедуры обновления *LiveUpdate* или сканирования на вирусы. Способ остановки выполнения встроенного ПО прибора описан в руководстве по эксплуатации прибора.

4.1.3 Отключение автоматического обновления и сканирования на вирусы

Для выполнения процедуры обновления Symantec LiveUpdate необходимо подсоединение к сети Интернет и наличие прав администратора. Обновления загружаются с сервера Symantec или с прокси-сервера вашей компании. Следует связаться с вашим отделом информационных технологий или системным администратором, чтобы получить сведения о политике информационной безопасности вашей компании.

Во избежание ухудшения производительности прибора следует настроить функцию обновления «LiveUpdate» и функцию сканирования по требованию «Scans to be executed on demand». Дважды щелкнуть на значке программы Norton AntiVirus в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно:



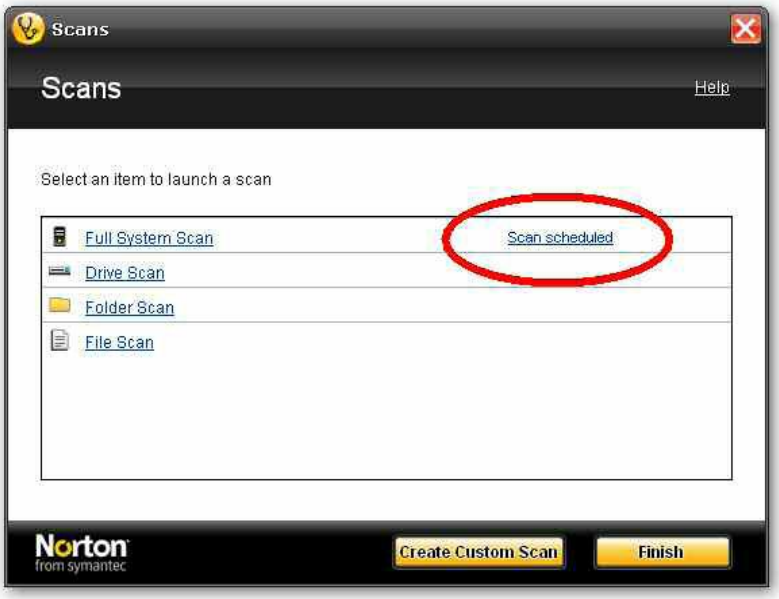
Выбрать вкладку **Settings** для настройки функций обновления и сканирования:

Отключить функцию автоматического обновления **Automatic LiveUpdate** и функцию быстрых обновлений **Pulse Updates** в диалоговом окне компьютерных настроек **Computer Settings**:

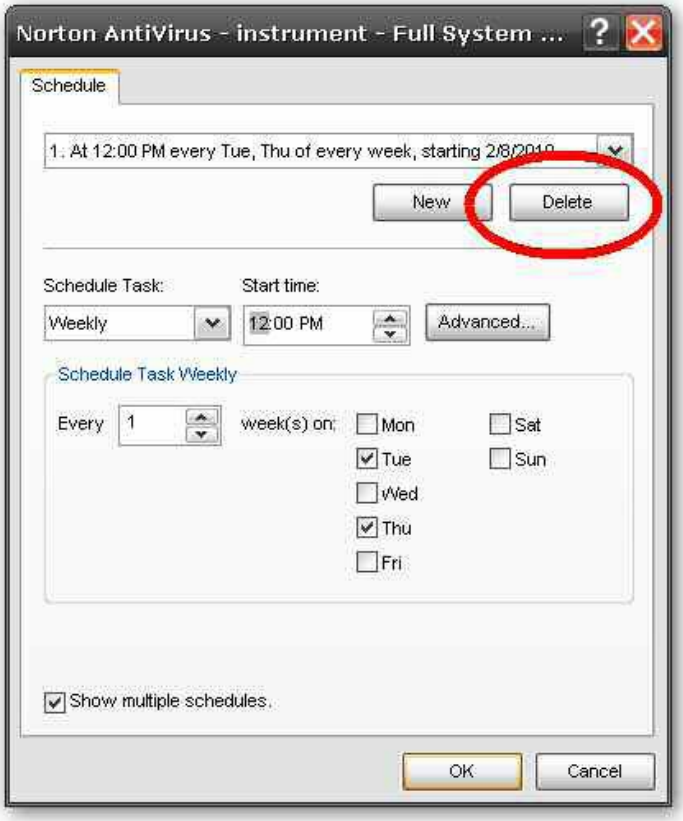
Сохранить настройки нажатием кнопки **OK**.

Последний этап настройки – отключение режима автоматического сканирования на вирусы. Вызвать главное диалоговое окно (см. описание выше) и нажать кнопку запуска пользовательского сканирования **Run Custom Scan**.

Выбрать команду сканирования по расписанию **Scan scheduled** для того, чтобы изменить список запланированных сканирований на вирусы:

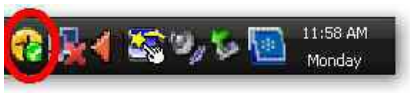


В диалоговом окне запланированных сканирований удалять записи до тех пор, пока раскрывающийся список не опустеет. Таким образом будут отключены все процедуры автоматического сканирования на вирусы:



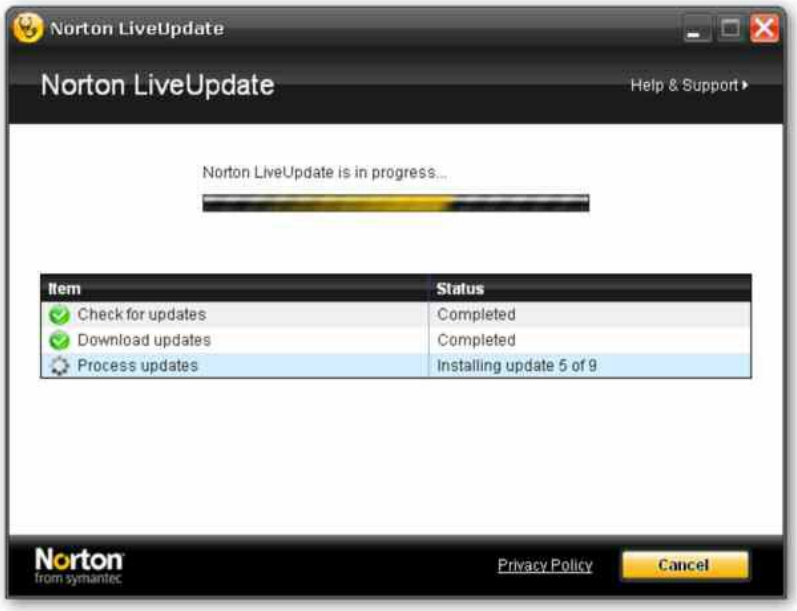
4.1.4 Обновление антивирусных баз и сканирование на вирусы по требованию

Для того чтобы на приборе запустить процедуру LiveUpdate обновления антивирусных баз и антивирусного ПО, необходимо подсоединение к сети Интернет. Дважды щелкнуть на значке программы Norton AntiVirus в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно программы:



Запустить процедуру обновления командой **Run LiveUpdate**:

По завершении процедуры обновления LiveUpdate нажать кнопку **OK**.



После того, как антивирусные базы были обновлены, можно запустить процедуру сканирования на вирусы.

Для того чтобы запустить процедуру сканирования, в главном диалоговом окне следует выбрать команду **Scan Now**:

В следующем диалоговом окне могут быть выбраны три варианта сканирования:

Могут быть просканированы наиболее часто заражаемые области (**Quick Scan**), выполнено полное сканирование прибора (**Full System Scan**), или запущено выборочное сканирование дисков, папок и файлов (**Custom Scan**).

По завершении процедуры сканирования следует нажать кнопку **Finish**, чтобы закрыть диалоговое окно сканирования.

4.2 Программа Kaspersky® Anti-Virus 2010

В данном разделе описана установка, настройка и использование антивирусного ПО Kaspersky Anti-Virus 2010 в приборах компании R&S.

4.2.1 Установка программы

Установить на прибор программу Kaspersky Anti-Virus 2010 в соответствии с описанием программного руководства.

По окончании установки следует запустить программу Kaspersky Anti-Virus 2010 для того, чтобы соединиться с сервером компании Kaspersky и получить последние описания вирусов и программные обновления.

4.2.2 Системные требования

Для установки и работы с ПО Kaspersky Anti-Virus 2010 должны выполняться следующие требования:

- 300 Мбайт свободного пространства на жестком диске прибора
- 256 Мбайт оперативной памяти
- ОС Windows XP SP2 и выше

Убедиться, что на вашем приборе компании R&S установлена версия ОС не ниже Windows XP SP2. Способ проверки текущей версии ОС описан в руководстве по эксплуатации прибора. Если прибор работает под управлением ОС более ранней версии, рекомендуется связаться с вашим представительством компании R&S на предмет возможного обновления ОС. Для многих приборов компания R&S предоставляет DVD-диск восстановления с последней версией ОС, предназначенный для полного восстановления данных на жестком диске прибора.

Во время выполнения процедуры обновления антивирусных баз / программы или сканирования на вирусы в приборе выполняются два процесса (оба с именем **avp.exe)**, которые занимают **до 320 Мбайт** памяти.

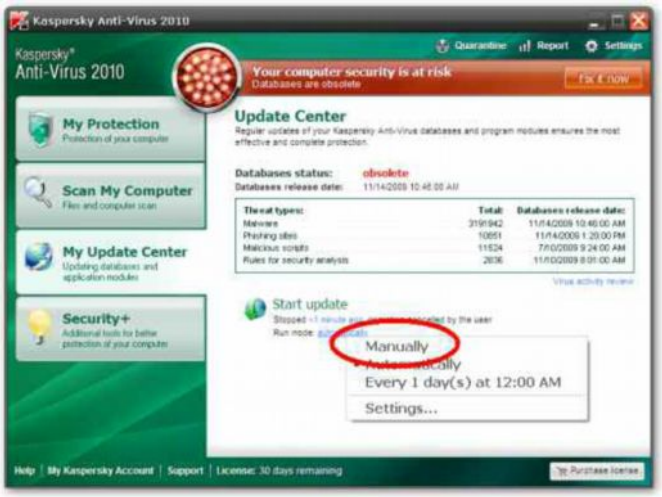
Таким образом, компания Rohde & Schwarz рекомендует останавливать встроенное ПО прибора перед запуском процедуры обновления или сканирования на вирусы. Способ остановки выполнения встроенного ПО прибора описан в руководстве по эксплуатации прибора.

4.2.3 Отключение автоматического обновления и сканирования на вирусы

Для запуска программы Kaspersky Anti-Virus 2010 необходимо подсоединение к сети Интернет и наличие прав администратора. Обновления загружаются с сервера Kaspersky или с прокси-сервера вашей компании. Следует связаться с вашим отделом информационных технологий или системным администратором, чтобы получить сведения о политике информационной безопасности вашей компании.

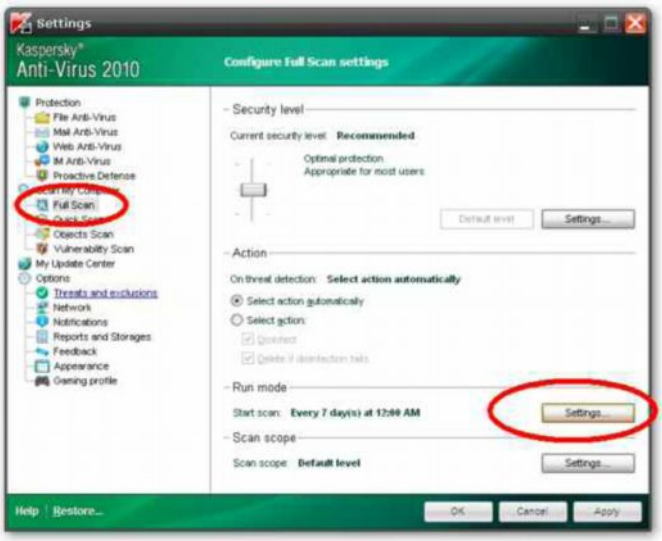
Во избежание ухудшения производительности прибора следует настроить выполнение обновлений антивирусных баз и сканирования на вирусы в режим «по требованию». Дважды щелкнуть на значке программы Kaspersky Anti-Virus в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно:

Выбрать вкладку центра обновления **My Update Center**. Чтобы отключить автоматическое обновление антивирусных баз / программы, выбрать пункт ручного режима **Manually** в меню **Start update ⇨ Run mode**:

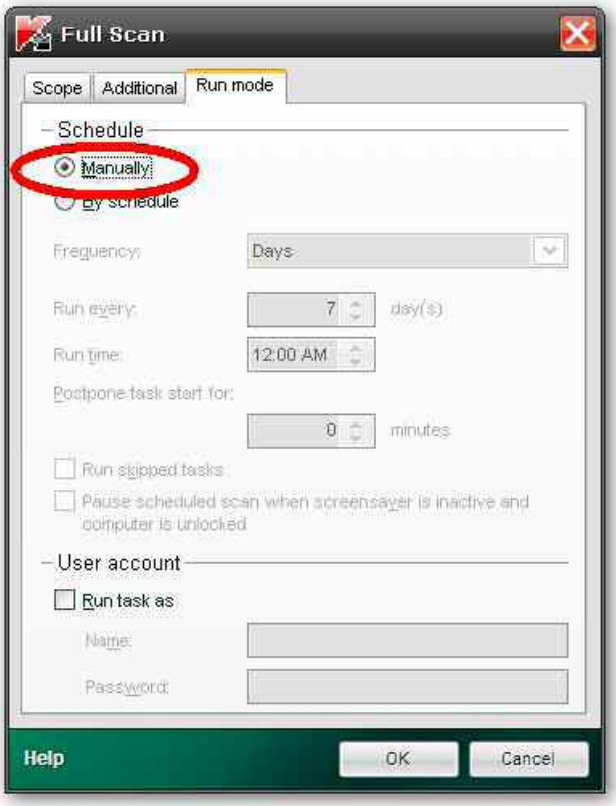


Чтобы настроить автоматическое сканирование на вирусы, выбрать пункт **Settings** в верхнем правом углу главного диалогового окна программы:

Выбрать режим полного сканирования **Full Scan** в левой панели навигации и нажать кнопку **Settings** для перехода к настройке режима выполнения *Run Mode*:



Выбрать ручной режим **Manually** в панели запланированных сканирований **Schedule** и нажать кнопку **OK**,чтобы подтвердить отключение автоматического режима сканирования на вирусы:



4.2.4 Обновление антивирусных баз и сканирование на вирусы по требованию

Для того чтобы на приборе запустить процедуру обновления антивирусных баз и антивирусного ПО, необходимо подсоединение к сети Интернет. Дважды щелкнуть на значке программы Kaspersky Anti-Virus в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно программы:

Чтобы запустить процедуру обновления, в главном диалоговом окне с левой стороны выбрать вкладку **My Update Center**, а затем выбрать команду **Start Update**:

Чтобы запустить процедуру сканирования на вирусы, в главном диалоговом окне с левой стороны выбрать вкладку **Scan My Computer**, а затем выбрать режим полного сканирования системы **Start Full Scan**:

Также может быть выбран режим быстрого сканирования **Quick Scan** или режим выборочного сканирования **Objects Scan**.

4.3 Программа Microsoft® Security Essentials

В данном разделе описана установка, настройка и использование антивирусного ПО Microsoft Security Essentials в приборах компании R&S.

4.3.1 Установка программы

Установить на прибор программу Microsoft Security Essentials в соответствии с описанием программного руководства. Для завершения установки не требуется соединения с сетью Интернет.

По окончании установки программа Microsoft Security Essentials попытается соединиться с сервером компании Microsoft для того, чтобы получить последние описания вирусов и программные обновления. Чтобы отменить эти действия следует отключить (снять флажок) функцию **Scan my computer for potential threats** и нажать кнопку **Finish** для завершения установки.

4.3.2 Системные требования

Для установки и работы с ПО Microsoft Security Essentials должны выполняться следующие требования:

- 300 Мбайт свободного пространства на жестком диске прибора
- 256 Мбайт оперативной памяти
- ОС Windows XP SP2 и выше

Убедиться, что на вашем приборе компании R&S установлена версия ОС не ниже Windows XP SP2. Способ проверки текущей версии ОС описан в руководстве по эксплуатации прибора. Если прибор работает под управлением ОС более ранней версии, рекомендуется связаться с вашим представительством компании R&S на предмет возможного обновления ОС. Для многих приборов компания R&S предоставляет DVD-диск восстановления с последней версией ОС, предназначенный для полного восстановления данных на жестком диске прибора.

Во время выполнения процедуры обновления антивирусных баз / программы или сканирования на вирусы в приборе выполняются два процесса (**MsMpEng.exe** и **msseces.exe**), которые занимают **до 110 Мбайт** памяти.

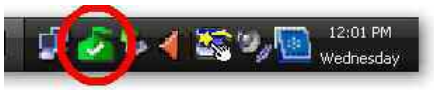
Таким образом, компания Rohde & Schwarz рекомендует останавливать встроенное ПО прибора перед запуском процедуры обновления или сканирования на вирусы. Способ остановки выполнения встроенного ПО прибора описан в руководстве по эксплуатации прибора.

4.3.3 Отключение автоматического сканирования на вирусы

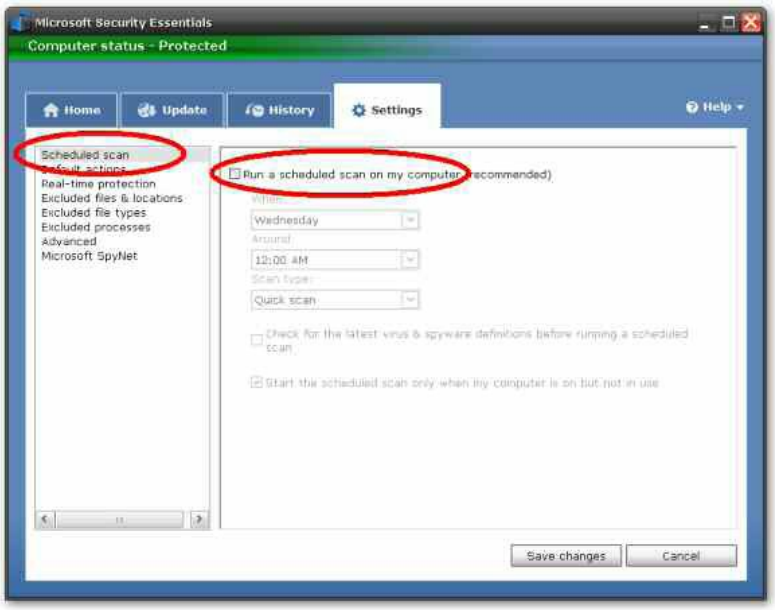
Для запуска программы Microsoft Security Essentials необходимо подсоединение к сети Интернет и наличие прав администратора.

Примечание – *Обновления антивирусных баз загружаются с сервера Microsoft автоматически, если используемые базы старее 24 часов. Отмена данного процесса автоматического обновления не предусмотрена. Кроме того, ПО Microsoft Security Essentials не может быть настроено для работы с прокси-сервером вашей компании.*

Во избежание ухудшения производительности прибора следует настроить выполнение сканирования на вирусы в режим «по требованию». Дважды щелкнуть на значке программы Microsoft Security Essentials в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно:



Выбрать вкладку настроек **Settings** и режим запланированных настроек **Scheduled scan** в левой части навигационной панели. Отменить выбор функции **Run a scheduled scan…** для того, чтобы отключить режим автоматического сканирования на вирусы.

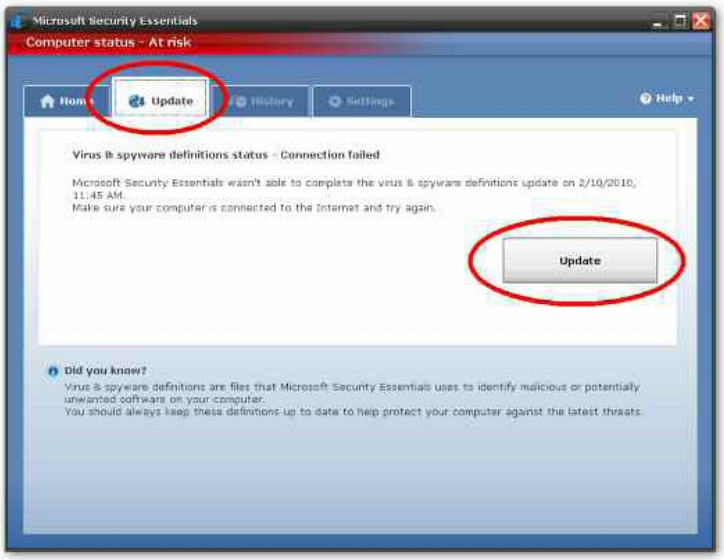


Сохранить конфигурацию с помощью кнопки **Save changes**.

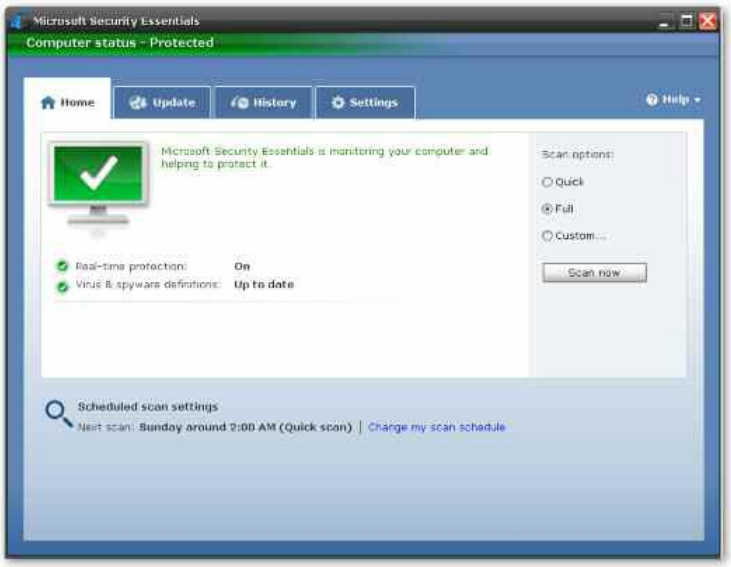
4.3.4 Обновление антивирусных баз и сканирование на вирусы по требованию

Для того чтобы на приборе запустить процедуру обновления антивирусных баз и антивирусного ПО, необходимо подсоединение к сети Интернет. Дважды щелкнуть на значке программы Microsoft Security Essentials в области уведомлений панели задач, чтобы вызвать на экран главное диалоговое окно программы:

Выбрать вкладку **Update** в главном диалоговом окне, затем нажать кнопку **Update** для того, чтобы запустить процедуру обновления:



Чтобы запустить процедуру сканирования на вирусы, в главном диалоговом окне выбрать вариант полного сканирования системы **Full Scan**, а затем нажать кнопку **Scan now**:



Также может быть выбран режим быстрого сканирования **Quick Scan** или режим выборочного сканирования **Objects Scan**.

4.4 Сканирование прибора с флэш-накопителя USB

Некоторые приборы не обладают достаточным для установки антивирусного ПО объемом ресурсов. Для таких приборов сканирование на вирусы может быть выполнено непосредственно с флэш-накопителя USB.

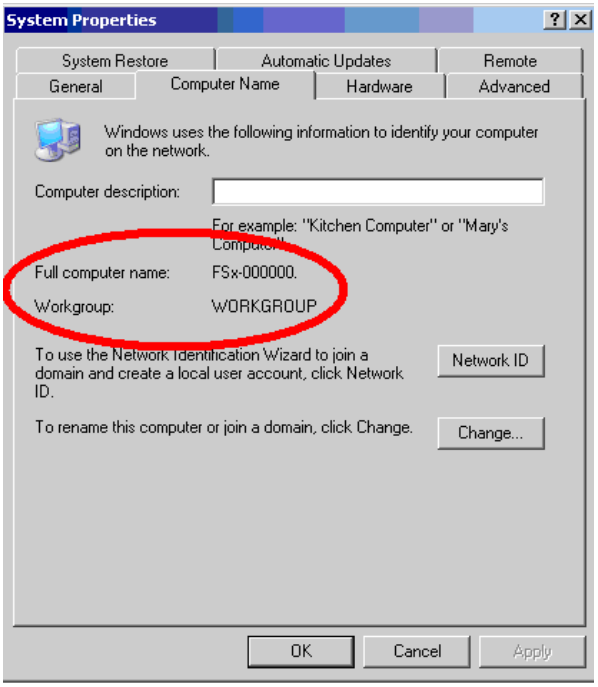
4.5 Сканирование приборов с другого компьютера

Перед выполнением сканирования на вирусы с помощью антивирусного ПО, установленного на другом компьютере, сканируемый прибор необходимо сделать видимым в сети в качестве сетевого диска.

Примечание – Удаленное сканирование жестких дисков прибора имеет некоторые ограничения, его следует использовать только в случаях, если другие возможности не доступны: могут быть просканированы только видимые файлы, память и выполняющиеся процессы не сканируются, поэтому вредоносный руткит может полностью скрыть свою деятельность.

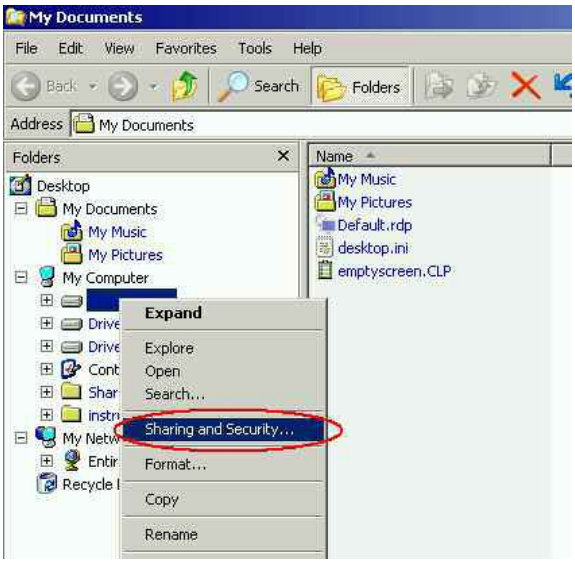
4.5.1 Общий доступ к дискам прибора

Подсоединить прибор к локальной сети. Проверить компьютерное имя прибора (Full computer name) и его рабочую группу (Workgroup). (В дальнейшем данная информация понадобится для сканирования этого прибора с другого компьютера). Чтобы просмотреть данные настройки следует открыть диалоговое окно свойств системы **Windows Start ⇨ Control Panel ⇨ System** и выбрать вкладку **Computer Name**:

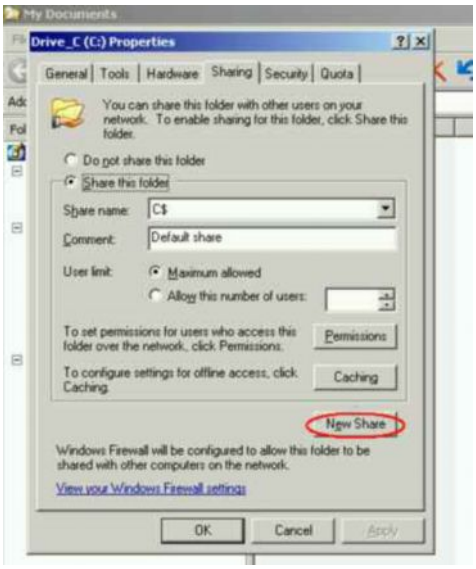


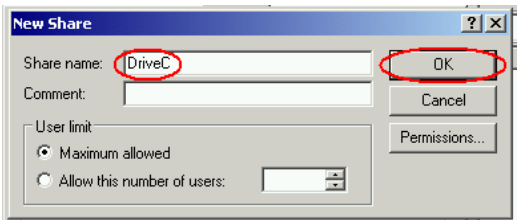
В данном случае, компьютерное имя прибора *FSx-000000*, он входит в рабочую группу *WORKGROUP*.

Запустить на приборе проводник Windows (Windows Explorer) и раскрыть папку **My Computer** для просмотра всех имеющихся в системе дисков. Щелкнуть правой кнопкой мыши на диске *Drive C:*, чтобы открыть контекстное меню, и выбрать команду **Sharing and Security**:



В открывшемся диалоговом окне нажать кнопку **New Share** и ввести имя общего ресурса, например, "DriveC", а затем подтвердить ввод нажатием кнопки OK.





Символ для диска *Drive C:* теперь изменится на символ общего диска:

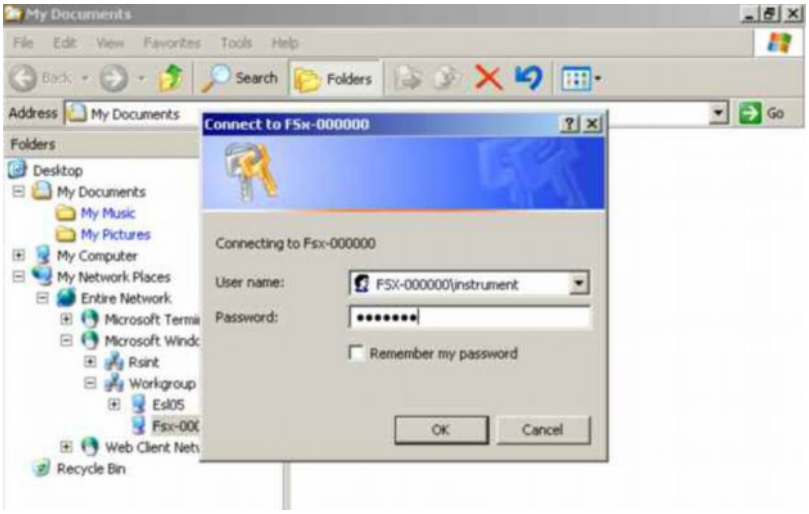
Повторить описанную процедуру для любого другого диска (например, для дисков D: и E: прибора). Таким образом, все диски прибора будут сделаны доступными для удаленного сканирования на вирусы.

4.5.2 Подключение сетевых дисков и сканирование на вирусы

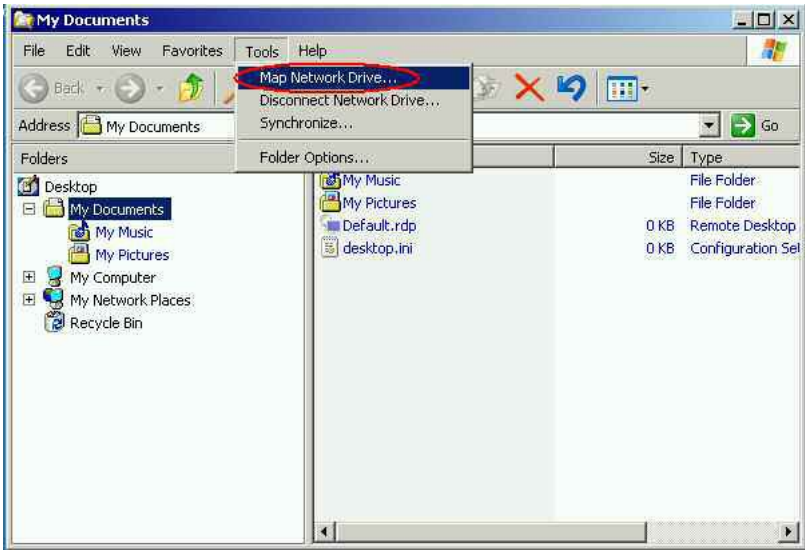
Открыть проводник Windows на вашем компьютере и раскрыть папки **My Network Places ⇨ Entire Network ⇨ Microsoft Windows Network ⇨ Workgroup** (Мое сетевое окружение ⇨ Вся сеть ⇨ Сеть Microsoft Windows ⇨ Workgroup).

Следует иметь в виду, что рабочая группа **Workgroup** может иметь другое название в вашей сетевой конфигурации.

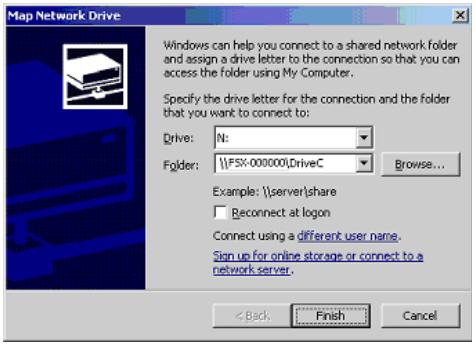
Щелкнуть по компьютерному имени прибора, который будет сканироваться, например, здесь это *FSx-000000*. Будет выдан запрос на ввод имени пользователя и пароля. Ввести имя пользователя **User Name** и пароль **Password** – их значения см. в руководстве по эксплуатации прибора.



Папки прибора будут показаны в правой части окна. В строке меню выбрать меню **Tools** (Сервис), а затем пункт **Map Network Drive…**(Подключить сетевой диск…)



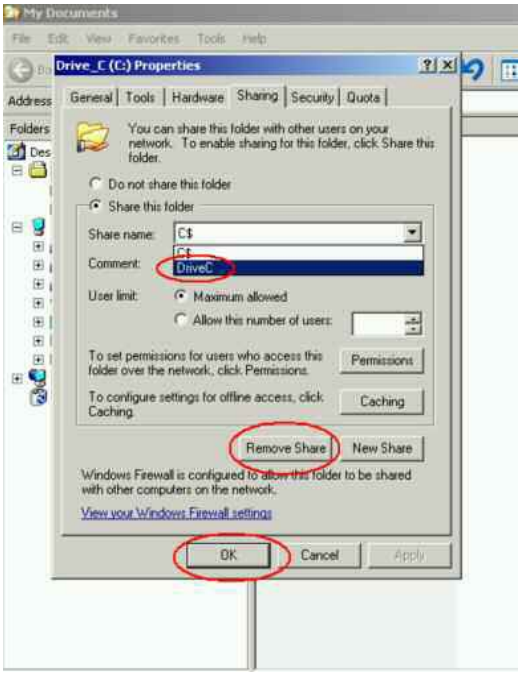
В диалоговом окне **Map Network Drive** (Подключение сетевого диска) назначить первый общий диск (например, диск «DriveC» прибора) в качестве сетевого диска (например, диска «N:» на компьютере управления). Для того чтобы найти полное сетевое имя общего диска (например, «\\FSX-000000\DriveC») в дереве сети, можно воспользоваться кнопкой **Browse** (Обзор). Нажать кнопку **Finish** (Готово) для завершения подключения сетевого диска. В рассмотренном примере диск C: прибора сделан сетевым диском N: на компьютере управления.



Повторить описанные действия для любых других жестких дисков прибора и назначить им свободные имена дисков на компьютере управления.

Чтобы выполнить сканирование жесткого диска прибора на вирусы, следует запустить антивирусное ПО на компьютере управления. Выбрать один из сетевых дисков прибора и запустить сканирование. Описание процедуры сканирования сетевых дисков см. в руководстве по антивирусному ПО.

Для того чтобы вернуть прибор в исходное состояние, следует отменить общий доступ к дискам прибора: Запустить на приборе проводник Windows и раскрыть папку **My Computer** для просмотра всех имеющихся в системе дисков. Щелкнуть правой кнопкой мыши на диске *Drive C:*, чтобы открыть контекстное меню. Выбрать вкладку **Sharing** в диалоговом окне свойств диска.



Развернуть список имен **Share name** и выбрать значение «DriveC», затем нажать кнопку **Remove Share** или установить кнопку-переключатель в позицию **Do not share this folder**. Наконец, нажать кнопку **OK**, чтобы отменить общий доступ к диску.

В случае необходимости повторить описанные действия для любых других общих дисков прибора.

5 Исправления и обновления ОС Windows

Компания Microsoft регулярно выпускает обновления для системы безопасности и другие исправления для защиты операционных систем семейства Windows. Они распространяются через веб-сайт Microsoft Update и связанный с ним сервер обновлений. Приборы, использующие ОС Windows, особенно подключенные к сети, следует обновлять регулярно.

Следует иметь в виду, что новый сервис Microsoft Update заменил сервис Windows Update, который был предназначен только для продуктов на базе Windows.

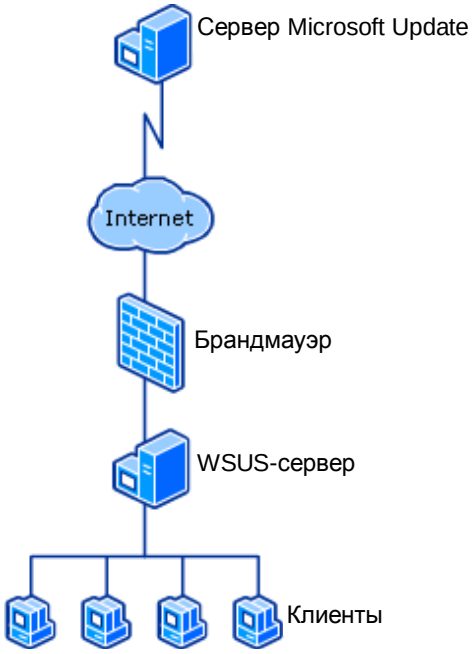
В следующих разделах описана установка агента обновления Windows Update Agent и его настройка. Агент позволит загружать и устанавливать на прибор новейшие исправления и обновления ОС Windows.

Убедиться, что на вашем приборе компании R&S установлена версия ОС не ниже Windows XP SP2. Способ проверки текущей версии ОС описан в руководстве по эксплуатации прибора. Если прибор работает под управлением ОС более ранней версии, рекомендуется связаться с вашим представительством компании R&S на предмет возможного обновления ОС. Для многих приборов компания R&S предоставляет DVD-диск восстановления с последней версией ОС, предназначенный для полного восстановления данных на жестком диске прибора.

Примечание – НЕ рекомендуется обновлять версию ОС прибора с SP2 на SP3 с помощью сервиса Microsoft Update или ручной установкой автономного пакета обновлений. Для большинства приборов необходимо использовать функцию полного восстановления ОС.

Обычно для приборов, использующих сервис Microsoft Update, реализуются два возможных сценария:

- Приборы имеют доступ в сеть Интернет и загружают обновления непосредственно с сервера Microsoft Update.
- Приборы загружают обновления с сервера обновлений вашей компании.



Во втором случае внутри корпоративной сети системные администраторы настраивают сервер, на котором выполняется служба обновлений Windows Server Update Services (WSUS), которая синхронизирует содержание обновлений с сервером Microsoft Update и распространяет обновления на клиентские компьютеры и приборы.

5.1 Установка и настройка агента обновлений Windows Update Agent

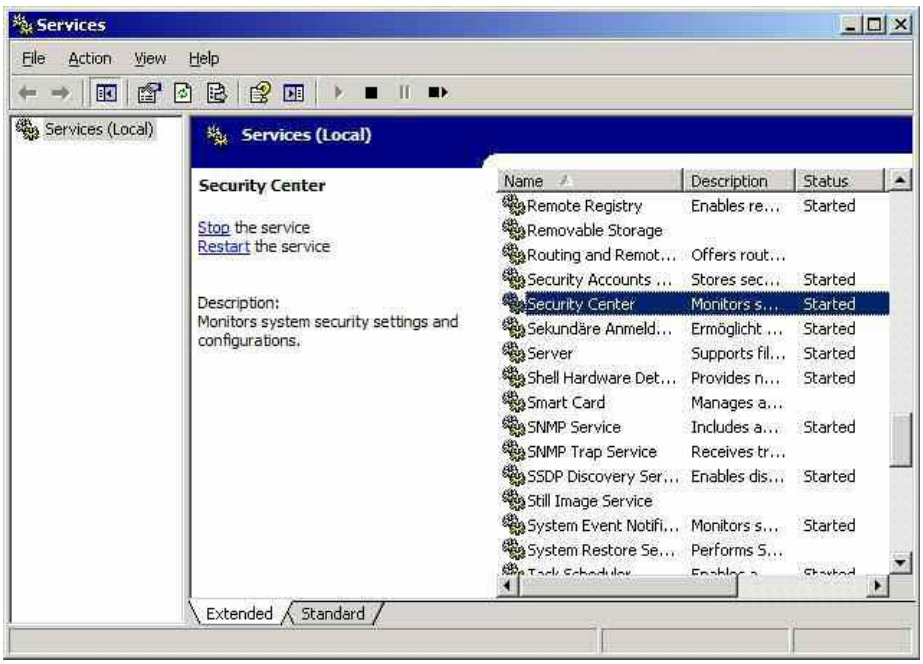
Большинство приборов компании R&S работают под управлением операционной системы Windows XP Embedded, представляющей собой специализированную версию ОС Windows XP Professional. ОС данного типа подогнана и оптимизирована под требования конкретных приборов. Следовательно, во многих случаях, на такие приборы службу обновлений Windows необходимо устанавливать отдельно.

Загрузить программу установки агента обновлений **WindowsUpdateAgent30-x86.exe** с веб-сайта Microsoft http://go.microsoft.com/fwlink/?LinkID=100334 и скопировать ее на флэш-накопитель USB. Процедура установки достаточно проста и не требует выбора каких-либо специальных опций.

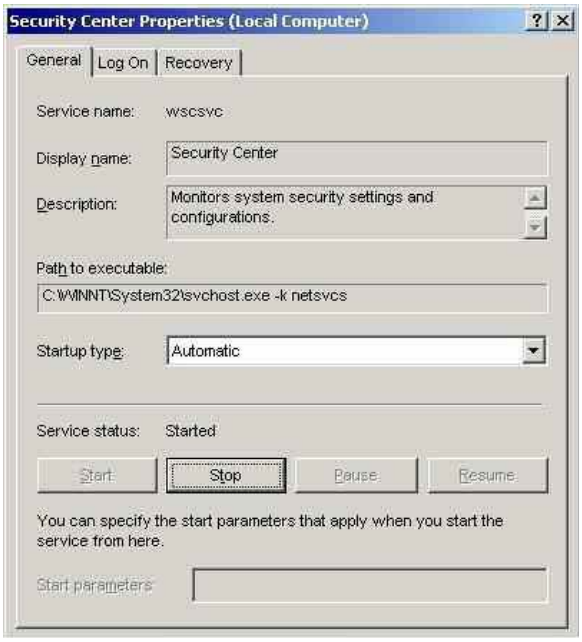
Ниже перечислены этапы установки агента обновлений Windows:

- Нажать CTRL + ESC или щелкнуть на кнопке **Start**, чтобы открыть стартовое меню Windows, и запустить проводник Windows (Windows Explorer).
- На флэш-накопителе USB выбрать каталог, в котором находится программа установки агента обновлений Windows.
- Запустить установку двойным щелчком мыши на EXE-файле.
- Прочитать и принять лицензионное соглашение, нажав кнопку *Next*.
- Следовать инструкциям мастера установки, чтобы завершить установку агента обновлений.

Для конфигурирования настроек агента обновлений Windows следует открыть панель управления **Windows Start ⇨ Control Panel**, а затем список служб **Administrative Tools ⇨ Services** и дважды щелкнуть на службе **Security Center**, чтобы открыть диалоговое окно настроек:



Выбрать автоматический **Automatic** тип запуска (Startup Type) и нажать кнопку **Start**, чтобы запустить службу:



Нажать **OK**, чтобы завершить процедуру настройки.

5.2 Настройка автоматического обновления

ОС Windows может быть настроена на установку важных обновлений сразу после их выхода с помощью службы автоматического обновления. Необязательные дополнения при этом не загружаются и не устанавливаются.

Чтобы запустить режим автоматического обновления, следует перейти к окну **Windows Start ⇨ Control Panel ⇨ Security Center**. В открытом диалоговом окне выбрать команду **Turn on Automatic Updates**.

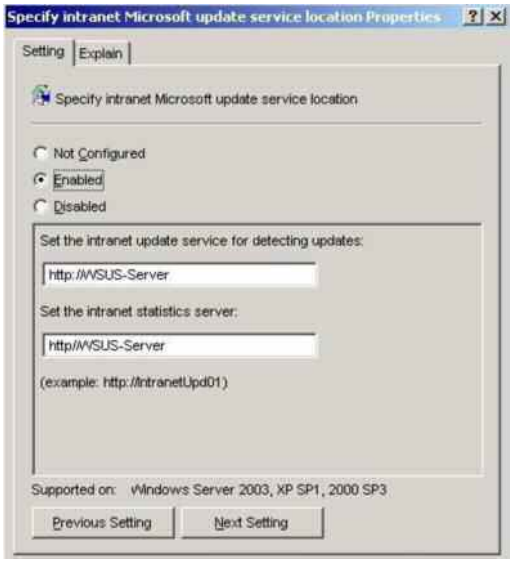
Режим автоматического обновления ОС прибора будет активирован.

5.3 Приборы, подсоединенные к серверу обновлений Windows Update Server

Во многих компаниях используют сервер обновлений Windows (WSUS-сервер), работающий в корпоративной сети. Если прибор подсоединен к локальной сети, то он может быть настроен на использование WSUS-сервера для получения обновлений Windows. Следует связаться с вашим отделом информационных технологий или системным администратором, чтобы настроить конфигурацию обновления прибора в соответствии с политикой информационной безопасности вашей компании.

Для того чтобы осуществлять управление или изменение настроек WSUS-клиента на приборе, следует открыть окно **Windows Start ⇨ Run** и ввести команду **gpedit.msc** для запуска редактора групповых политик. Перейти к шаблону **Computer Configuration ⇨ Administrative Templates ⇨ Windows Components ⇨ Windows Updates**. Просмотреть список и дважды щелкнуть на настройке **Specify intranet Microsoft update service location**, чтобы открыть диалоговое окно настроек:

Сначала выбрать пункт **Enabled**, затем указать имя сервера обновлений в локальной сети компании, который будет использован для получения обновлений:



Примечание – Убедиться, что режим автоматического обновления включен (см. раздел 5.1).

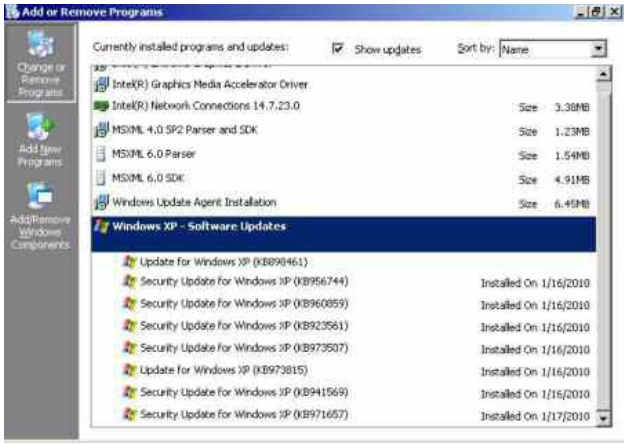
5.4 Настройка автоматического обновления

Возможна достаточно гибкая настройка режима автоматического обновления. Например, получение обновлений может настроено на заданный день и время, могут быть включены уведомления пользователя и т.д. Указанные настройки могут быть выполнены в окне **Windows Start ⇨ Control Panel ⇨ Automatic Updates:**

Для приборов компании Rohde & Schwarz настоятельно рекомендуется использовать режим уведомления «Notify me…», в котором перед загрузкой и установкой обновлений требуется получение подтверждения пользователя. Загрузка обновлений и их установка может привести к снижению производительности прибора и даже потребовать его перезагрузки. Следовательно, пользователю следует управлять процедурой обновления для того, чтобы она не выполнялась во время работы с прибором.

5.5 Просмотр установленных обновлений

Установленные обновления могут быть просмотрены в окне установки и удаления программ **Windows Start ⇨ Control Panel ⇨ Add or Remove Programs**:



Следует убедиться, что выбрана функция отображения обновлений **Show updates**.

6 Справочные документы и ссылки

- NSA Security papers
  http://www.nsa.gov/ia/guidance/security_configuration_guides/
- News about Security threats
  http://www.securityfocus.com/
- Microsoft Windows Update Agent – Download Link
  http://go.microsoft.com/fwlink/?LinkID=100334
- Microsoft Support: How to disable the Autorun functionality in Windows
  http://support.microsoft.com/kb/967715/en-us
- Microsoft Support: Troubleshooting Windows Firewall settings in Windows XP Service Pack 2 for advanced users
  http://support.microsoft.com/kb/875357/en-us

О компании Rohde & Schwarz
Rohde & Schwarz представляет собой независимую группу компаний, специализирующуюся на производстве электронного оборудования. Rohde & Schwarz является ведущим поставщиком контрольно-измерительных систем и приборов, оборудования для теле- и радиовещания, систем радиомониторинга и радиопеленгации, а также систем профессиональной радиосвязи специального назначения. Rohde & Schwarz успешно работает уже 75 лет, представительства и сервисные центры компании находятся в более чем 70 странах. Головной офис компании расположен в Мюнхене, Германия.

Приверженность делу охраны окружающей среды
- Энергосберегающие изделия
- Непрерывное усовершенствование в области экологической устойчивости
- Сертифицированная система экологического менеджмента ISO 14001

Контакты в регионах

США & Канада
США: 1-888-TEST-RSA (1-888-837-8772)
извне США: +1 410 910 7800
CustomerSupport@rohde-schwarz.com

Восточная Азия
+65 65 13 04 88
CustomerSupport@rohde-schwarz.com

Другие регионы
+49 89 4129 137 74
CustomerSupport@rohde-schwarz.com

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | D - 81671 München
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com