

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
СВЕРДЛОВСКОЙ ОБЛАСТИ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ
ОБЛАСТИ «КАМЫШЛОВСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И
ТРАНСПОРТА»

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К
ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ
МДК 02.01. УСТАНОВКА И НАСТРОЙКА АППАРАТНЫХ И
ПРОГРАММНЫХ СРЕДСТВ ДОСТУПА В СЕТЬ ИНТЕРНЕТ**
для студентов профессии 09.01.02 Наладчик компьютерных сетей

Составил:
Преподаватель Потапова О.А.
1 квалификационная категория

Камышлов
2015

АННОТАЦИЯ

Методические рекомендации по практическим работам для студентов профессии 09.01.02 Наладчик компьютерных сетей содержат материалы с заданиями по выполнению практических работ студентами по учебной дисциплине МДК 02.01. Установка и настройка аппаратных и программных средств доступа в сеть интернет.

Методические рекомендации, включают указания по выполнению практических работ по разделу 1. Пространства имен и разделу 2 Установка и настройка программного обеспечения серверов сети Интернет, а также список литературных и других источников информации, необходимых для выполнения практических работ.

СОДЕРЖАНИЕ

Тема: Распределения имен	4
Тема: DNS-в интернете.....	4
Тема: Изучение особенностей операционной системы для сервера.....	6
Тема: Аппаратные и программные требования для установки ОС	9
Тема: Ознакомление с этапами администрирования сервера и настройки групповых политик.....	11
Список источников	21
Заключение.....	22

Доступ к файлу page.htm, находящемуся на сервере book.ru, осуществляется по протоколу http. В таблице фрагменты адреса файла закодированы буквами от А до Ж. Запишите последовательность этих букв, кодирующую адрес указанного файла в сети Интернет.

- А) /
- Б) page
- В) ://
- Г) .ru
- Д) .htm
- Е) book
- Ж) http

Ответ:

Доступ к файлу lot.htm, находящемуся на сервере catalog.ru, осуществляется по протоколу http. В таблице фрагменты адреса файла закодированы буквами от А до Ж. Запишите последовательность этих букв, кодирующую адрес указанного файла в сети Интернет.

- А) /
- Б) ://
- В) lot
- Г) catalog
- Д) http
- Е) .htm
- Ж) .ru

Ответ:

Доступ к файлу book1.htm, находящемуся на сервере biblio.ru, осуществляется по протоколу http. В таблице фрагменты адреса файла закодированы буквами от А до Ж. Запишите последовательность этих букв, кодирующую адрес указанного файла в сети Интернет.

- А) ://
- Б) biblio
- В) http
- Г) .ru
- Д) .htm
- Е) book1
- Ж) /

Ответ:

Задание 2. Определение адреса сети

Зайдите в командную строку:
Пуск-Выполнить – cmd - ОК
Набираем команду Ipconfig – Enter

И мы видим IP – адрес, а также маску подсети.
Теперь попробуем определить адрес сети.

```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Administrator>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети 2 - Ethernet адаптер:
    DNS-суффикс этого подключения . . . :
    IP-адрес . . . . . : 192.168.0.2
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

Подключение по локальной сети - Ethernet адаптер:
    DNS-суффикс этого подключения . . . :
    IP-адрес . . . . . : 188.32.255.81
    Маска подсети . . . . . : 255.255.224.0
    Основной шлюз . . . . . : 188.32.224.1

C:\Documents and Settings\Administrator>_
```

В терминологии сетей TCP/IP маской сети называется двоичное число, определяющее, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети. Обычно маска записывается по тем же правилам, что и IP-адрес. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

По заданным IP-адресу узла и маске определите адрес сети.

IP –адрес узла: 142.9.199.145

Маска: 255.255.192.0

При записи ответа выберите из приведенных в таблице чисел четыре элемента IP-адреса и запишите в нужном порядке соответствующие им буквы, без использования точек.

A	B	C	D	E	F	G	H
0	9	16	64	128	142	192	224

«Определение адреса сети»

Тема: Изучение особенностей операционной системы для сервера

Цель работы: познакомиться с возможностями и особенностями серверных операционных систем.

Теоретический материал

Серверная операционная система, в отличие от пользовательской, предоставляет более широкий функционал для управления IT-инфраструктурой, программным обеспечением, установленным не только на сервере, но и на компьютерах пользователей сети, причём как внутренней, так и внешней.

Основная визуальная отличительная особенность любой серверной операционной системы – это возможность работать без графической оболочки (привычного большинству пользователей ПК интерфейса ОС). Наличие графической оболочки

операционной системы требует большего количества аппаратных ресурсов. Следовательно, серверные ОС, рассчитанные на эксплуатацию специалистами или, как минимум, «продвинутыми» пользователями, допускают возможность работать без графической оболочки, то есть непосредственно из файлового менеджера.

Многие серверы непосредственно на этапе производства «затачиваются» под определённые операционные системы. Так, например, **серверы HP** имеют сертификацию Microsoft, а также соответствующий набор инструментов для быстрого развёртывания операционной системы и быстрой интеграции серверного оборудования в IT-инфраструктуру предприятия. Однако, помимо серверных версий Microsoft Windows, существуют другие операционные системы. И какую именно ОС устанавливать на конкретный сервер, зависит не только от аппаратной архитектуры сервера, но и от конкретного функционального назначения вычислительной машины.

Серверные операционные системы Microsoft Windows Server 2003

ОС Windows Server 2003 (семейство NT), несмотря на давность выпуска, до сих пор остаётся довольно популярной в России.

Эта операционная система довольно универсальна, то есть подходит для инсталляции и на сервер баз данных, и на файловый сервер, и хостинговый, и др. Наиболее популярные приложения – контроллер доменов, сервер приложений для Microsoft .NET. Чтобы развернуть сервер под эти приложения, с ОС Windows Server 2003 не требуется устанавливать дополнительного программного обеспечения.

Интерфейс системы – простой и понятный, используется ролевая система доступа. Поэтому Windows Server 2003 чаще всего выбирают начинающие системные администраторы.

Серверная операционная система Windows Server 2003 имеет 4 версии, каждая из которых предназначена для IT-инфраструктуры определённого масштаба.

Windows Server 2008 R2

Windows Server 2008 R2 выпущена относительно недавно и на сегодняшний день она пока остаётся лидером по производительности среди серверных ОС.

Windows Server 2008 R2 идеально подходит для организации файлового сервера или виртуализированных сред. По сравнению с предыдущей версией ОС, здесь более «продвинутые» служба каталогов Active Directory и терминальный сервер. Собственно, и аппаратных ресурсов для этой системы требуется больше.

Windows Server 2012

Windows Server 2012 (или WS 8) — это первая версия серверной операционной системы Microsoft, не поддерживающая процессоры Itanium (собственно, их производство было прекращено ещё в 2002 году, поэтому для современных серверов это замечание неактуально).

Основные отличия от предыдущей ОС – усовершенствованный пользовательский интерфейс, напоминающий интерфейс ОС для персональных компьютеров Windows 8, модернизированный диспетчер задач, а также возможность переключаться между режимами отображения рабочего стола без необходимости перезагрузки. Также была добавлена новая роль администрирования - IP Address Management – для управления адресным пространством.

Также в серверной операционной системе Windows Server 2012 добавлена новая служба безопасности Dynamic Access Control.

Системы UNIX

Ubuntu Server 10.10

Ubuntu Server 10.10 – самая популярная серверная операционная система среди систем UNIX. Несмотря на то, Ubuntu Server имеет и более поздние релизы, чаще всего системными администраторами используется именно версия 10.10.

Это только с первого раза может показаться, что управление ИТ-инфраструктурой из-под системы с ядром Linux - это непонятно и очень трудно. На самом деле, пугает обычно именно отсутствие графического интерфейса, но к этому можно очень быстро привыкнуть. А настройка UNIX-подобных систем, как правило, протекает намного быстрее и проще, нежели ОС Windows.

Всё конфигурирование системы сводится к редактированию конфигурационных файлов.

Ubuntu Server 10.10 отлично подходит для серверов любого функционального назначения, при этом отличается высокими показателями надёжности и производительности (благодаря отсутствию графической оболочки).

CentOS 5.5

CentOS (аббр. Community ENTerprise Operating System) — также весьма популярная серверная операционная система для любителей всего проверенного и надёжного.

CentOS была операционной системой серверов проекта Cluster Compute Instance, запущенного Amazon.

Debian 6.0

Debian 6.0 отличается огромным количеством программного обеспечения, разрабатываемого энтузиастами и доступного для свободного скачивания. Программное обеспечение позволяет расширять функциональность сервера до достижения аппаратного предела последнего.

По удобству управления Дебиан, как считается, рассчитан для системных администраторов, уже имевших опыт работы с unix-подобными ОС. То есть эта система не для новичка.

Из ключевых функциональных особенностей Debian – уникальная система менеджмента пакетами – без переустановки, без перезагрузки сервера, без потери настроек.

Gentoo

Gentoo – одна из сложнейших в плане управления серверных операционных систем на ядре Linux. Однако при правильном развёртывании системы обеспечивает высочайшую производительность.

Сообщество пользователей Gentoo довольно многочисленно, и если вы решите использовать эту ОС, в сети легко будет найти поддержку и ответы на многочисленные вопросы, которые у вас могут возникнуть.

FreeBSD 8.2

FreeBSD 8.2 – серверная операционная система, идеальная для организации веб-сервера, благодаря мощному TCP/IP, поддерживающему промышленные стандарты сетевых протоколов NFS, SLIP, PPP, DHCP и NIS. Следовательно, сервер на FreeBSD можно легко интегрировать практически в любую ИТ-инфраструктуру.

На серверной платформе FreeBSD работают самые популярные поисковые системы (например, Yahoo).

При выборе FreeBSD вы также найдёте хорошую поддержку в сети среди энтузиастов-разработчиков.

Solaris

Solaris – серверная операционная система с графической оболочкой, до недавнего времени была бесплатной (пока её не выкупила у разработчика компания Oracle Corporation). Впрочем, существуют и бесплатные, некоммерческие версии программного обеспечения, но не предоставляющие возможности получить техподдержку производителя.

Solaris – одна из самых производительных ОС в мире.

На основании теоретического материалы заполните таблицу. Недостающие данные для заполнения таблицы найдите с использованием ресурсов сети Интернет:

Таблица 1. Особенности серверных операционных систем

Вид ОС	Название ОС	Преимущества	Недостатки
Серверные операционные системы Microsoft			
Системы UNIX			
Прочие системы			

Тема: Аппаратные и программные требования для установки ОС

Цель работы: Научиться устанавливать факт возможности использования ОС на персональном компьютере
Теоретический материал:

Системные требования

Ниже перечислены системные требования для Windows Server 2008 R2. Если компьютер не удовлетворяет минимальным требованиям, правильно установить продукт будет невозможно. Фактические требования зависят от конфигурации компьютера и устанавливаемых приложений и компонентов.

Процессор

Производительность процессора зависит не только от тактовой частоты процессора, но также от количества его ядер и от размера его кэша. Ниже перечислены требования к процессору для данного продукта.

Для успешной установки необходимо не менее 32 ГБ свободного места на диске. Дополнительное свободное место для системного раздела потребуется в любом из нижеперечисленных случаев.

- При установке системы по сети.
- Для компьютеров с ОЗУ более 16 ГБ может потребоваться больше места на диске для файлов подкачки, спящего режима и дампа.
- При установке системы Windows Server 2008 R2 на компьютер с процессором Itanium.

При определении минимального объема свободного места для установки операционной системы необходимо учесть несколько дополнительных факторов.

- Объем ОЗУ, который повлияет на дисковое пространство, необходимое для файлов подкачки, файлов спящего режима и файлов дампа.
- Требования к обслуживанию, в частности, планируется ли установка всех доступных обновлений, только критических обновлений или пакетов обновления, а также частота установки обновлений (ежемесячно, ежеквартально, с другой частотой).

- Планируемый срок службы сервера, поскольку необходимо предусмотреть увеличение объема системного раздела в течение долгого времени при установке всех обновлений.
- Планы по обновлению на следующие версии операционной системы, поскольку для установки новой системы вместо старой часто требуется больший объем дискового пространства, чем тот объем, который будет использоваться после завершения установки.
- Число и объем драйверов сторонних производителей и связанных с ними программных средств.

Задание:

Установите факт использования операционной системы Windows Server 2008 на персональном компьютере вашего рабочего места. Для этого внимательно изучите аппаратные требования к операционной системе и имеющуюся аппаратную конфигурацию вашего ПК. Сделайте выводы об использовании программного обеспечения.

Требования к ПК	Значение		Значение для вашего ПК
	минимальные	максимальные	
<i>Процессор</i>	64-разрядный процессор 1,4 ГГц (Для Windows Server 2008 R2 для компьютеров на базе процессоров Itanium требуется процессор Intel Itanium 2.)	-	
<i>ОЗУ</i>	512 МБ	32 ГБ (для Windows Server 2008 R2 Standard) или 2 ТБ (для Windows Server 2008 R2 Enterprise, Windows Server 2008 R2 Datacenter и Windows Server 2008 R2 для компьютеров на базе процессоров Itanium).	
<i>Требования к месту на диске</i>	32 ГБ	-	
<i>Другие требования</i>	DVD-дисковод		
	Монитор Super VGA (800 x 600) или с более высоким разрешением		
	Клавиатура и мышь Microsoft® (или другое совместимое указывающее устройство)		

	Доступ к Интернету (может потребоваться дополнительная оплата)	
--	--	--

Вывод об использовании:

Тема: Ознакомление с этапами администрирования сервера и настройки групповых политик

Цель работы: рассмотреть вариант настройки сервера с помощью мастера настройки безопасности

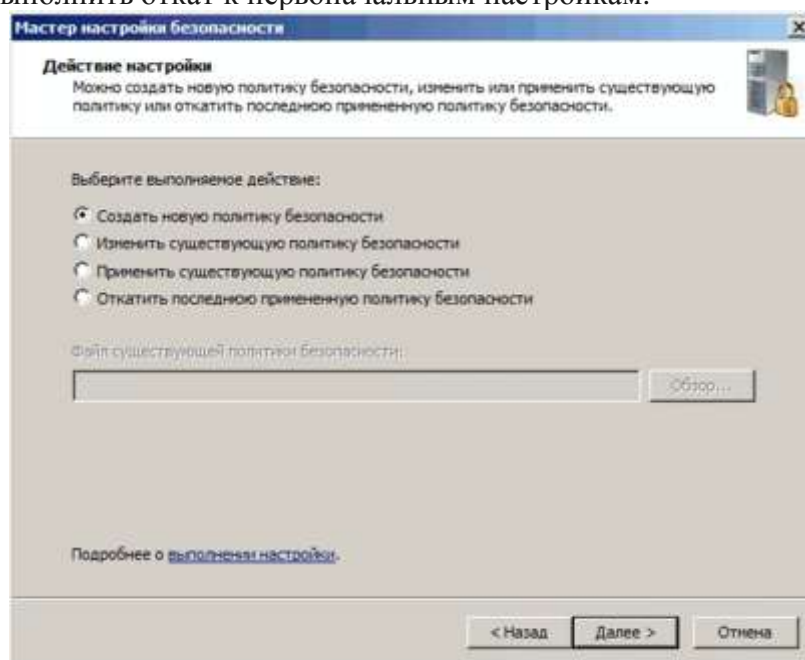
Правильный подход к безопасности подразумевает, что на сервере должны быть активированы только те службы, которые необходимы для выполнения сервером своих задач. Другими словами, *DHCP*-сервер должен отвечать только на запросы *DHCP*, а у *DNS*-сервера должен быть активирован только *DNS*. Мастер настройки безопасности (*Security Configuration Wizard, SCW*) позволяет отключить все неиспользуемые службы сервера за исключением тех, которые необходимы для выполнения специфических задач. Также *SCW* позволяет создавать шаблоны, которые затем могут быть экспортированы на другие сервера для автоматизации настройки безопасности.

ХОД РАБОТЫ

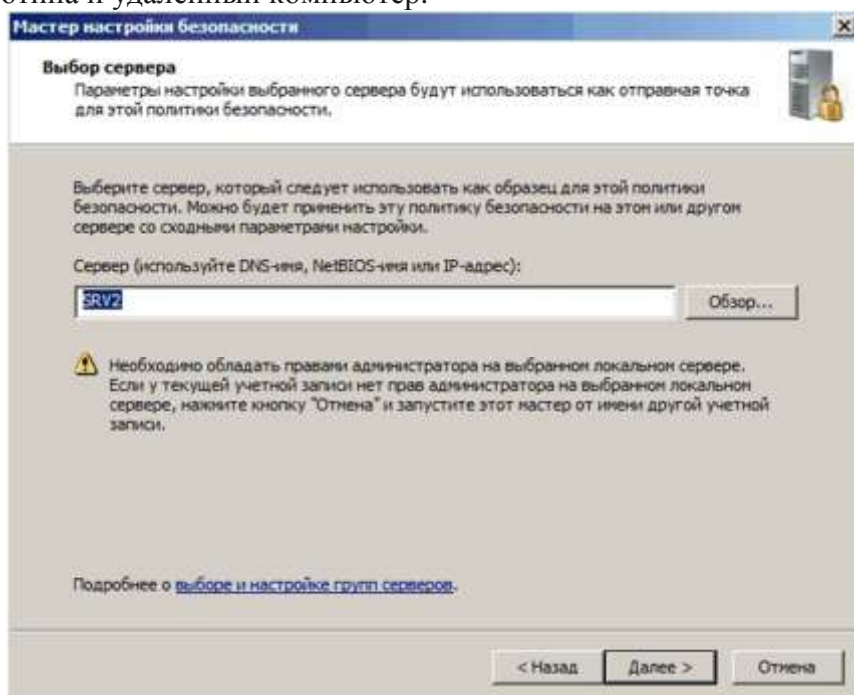
Мастер *SCW* можно запустить из окна Диспетчера сервера (*Server Manager*), или выбрав одноименную ссылку в окне Администрирование (*Administrative Tools*) в панели управления.

SCW необходимо использовать сразу после установки всех ролей и компонентов, которые должны иметься на сервере. Если предполагаются приложения сторонних производителей, их также следует установить до запуска *SCW*.

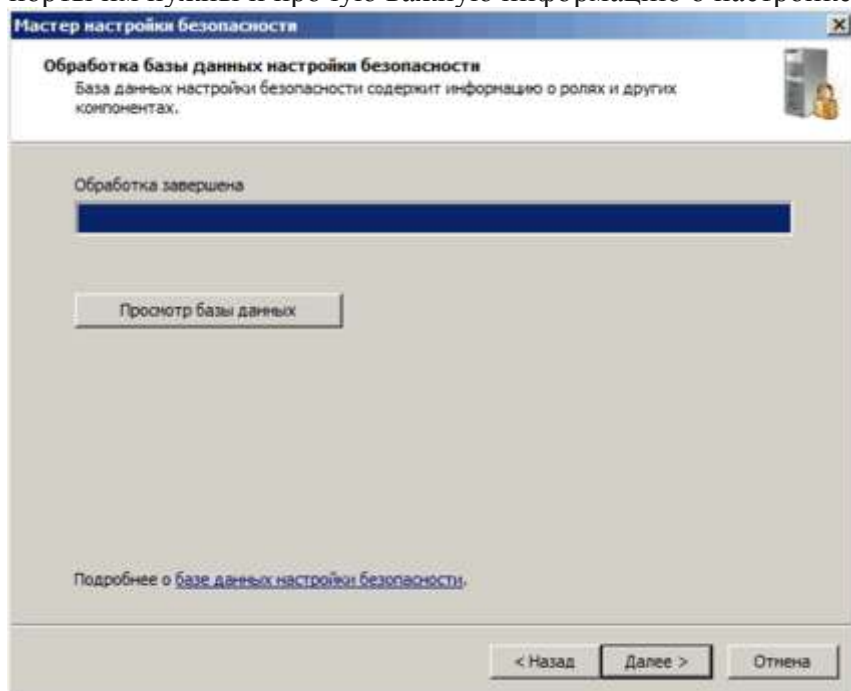
Работа мастера разделена на несколько этапов. Первый этап – это выбор того, хотите ли вы создать новую политику безопасности, изменить или применить существующую политику или откатить политику к первоначальным настройкам.



Для создания новой политики SCW должен проанализировать компьютер, определяя какие компоненты и роли тот поддерживает. При нажатии кнопки «Далее» мастер запрашивает, какой компьютер следует использовать как базовый вариант (прототип) для новой политики. Обычно стоит выбирать локальный компьютер, но можно использовать в качестве прототипа и удаленный компьютер.

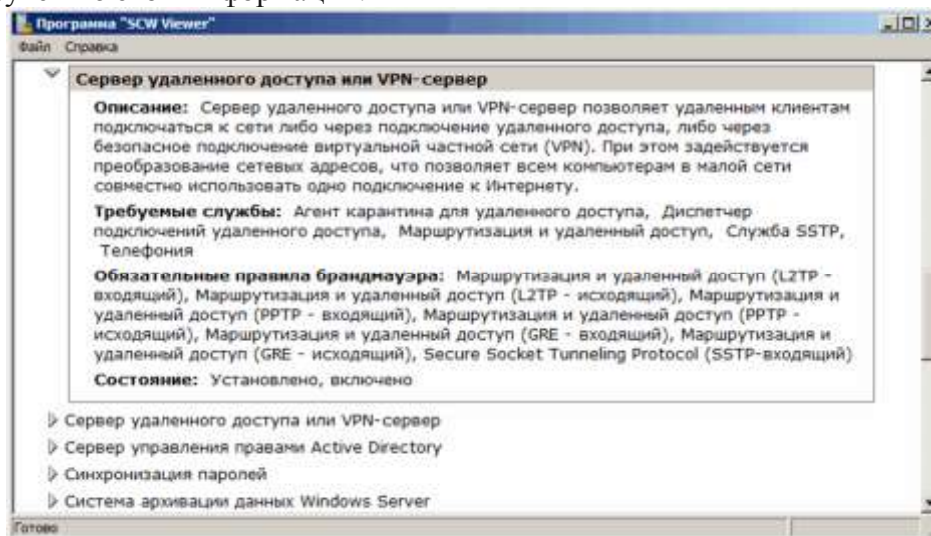


После указания компьютера начинается фаза анализа. В ней SCW формирует список установленных ролей и компонентов и сопоставляет его с базой данных. База данных содержит информацию о том, какие службы используются каждой ролью и компонентом, какие сетевые порты им нужны и прочую важную информацию о настройке.



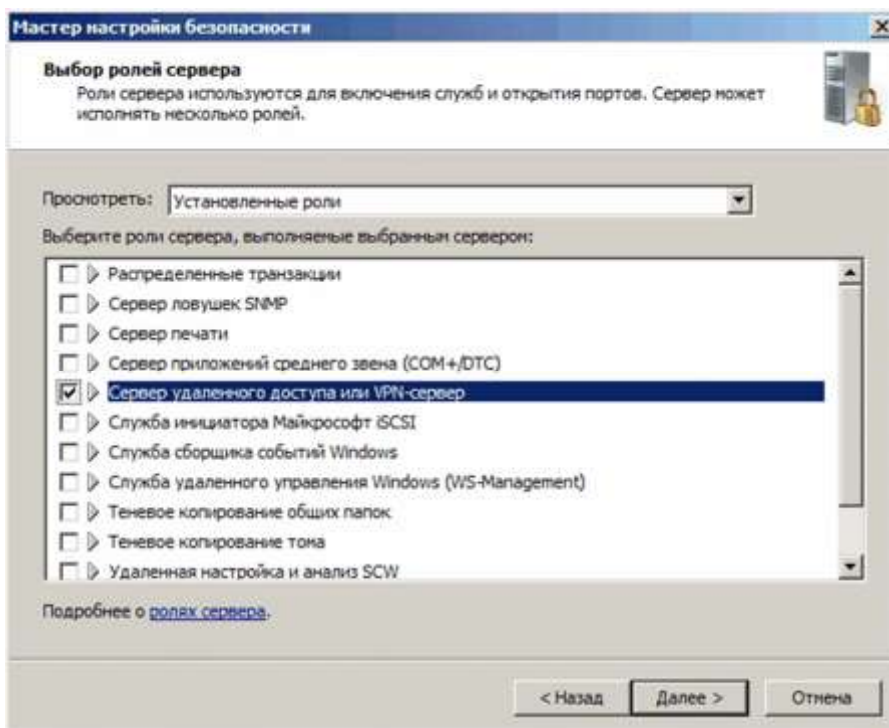
По завершении анализа можно нажать кнопку просмотра базы данных настроек, чтобы увидеть, что нашел SCW. Эти сведения открываются в SCW Viewer для чтения и предоставляют исчерпывающую информацию обо всех настройках сервера. Если вам

действительно интересно, что находится на вашем сервере, можете посвятить побольше времени изучению этой информации.

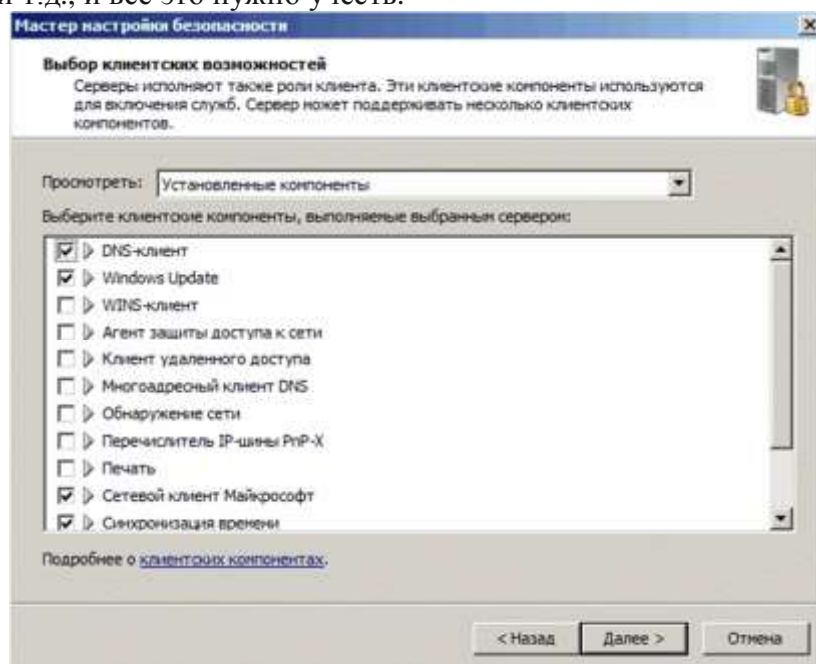


После анализа переходим непосредственно к настройке. Нажимаем кнопку «Далее» и попадаем в первый из четырех разделов SCW — настройку служб на основе ролей. Обратите внимание, что имеющиеся в SCW роли не совсем совпадают с ролями в мастере добавления ролей. SCW предлагает некоторые роли, не включенные в мастер добавления ролей.

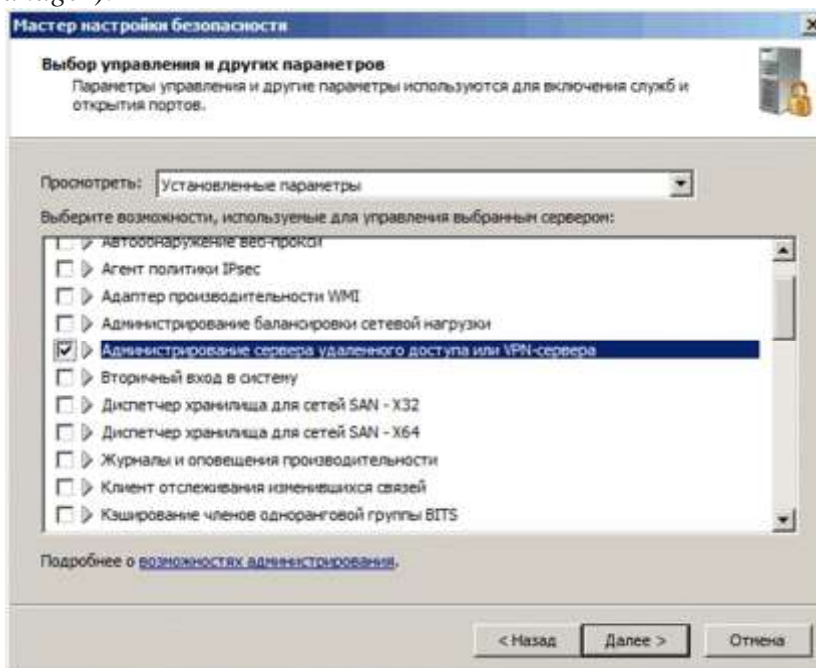
По умолчанию показываются установленные роли, то есть роли, которые сервер потенциально способен поддерживать без установки дополнительных компонентов. Выбранные роли – это роли, которые он поддерживает в настоящий момент. Также можно выбрать показ всех ролей, для чего просто укажите «Все роли» в раскрывающемся списке. Это может понадобиться при необходимости создать политику на сервере, на котором еще не установлены все необходимые роли. В любом случае, нам надо отметить только те роли, которые будет исполнять данный сервер (в нашем случае это сервер удаленного доступа).



Далее следует диалог выбора клиентских возможностей. Любой сервер является еще и клиентом, например обращается с запросами к *DNS*-серверу, получает обновления с сервера *WSUS* и т.д., и все это нужно учесть.



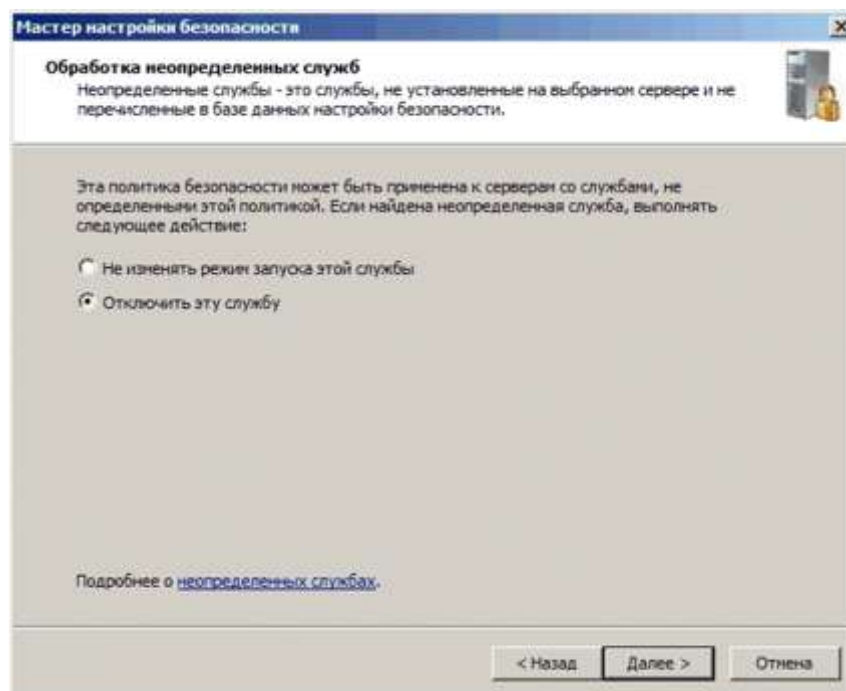
В следующем окне выбираем параметры управления сервером. Выбор включает оснастки, необходимые для управления выбранными ролями сервера. Кроме того, здесь можно разрешить удаленное управление сервером с помощью средств администрирования (напр. *Server Manager*).



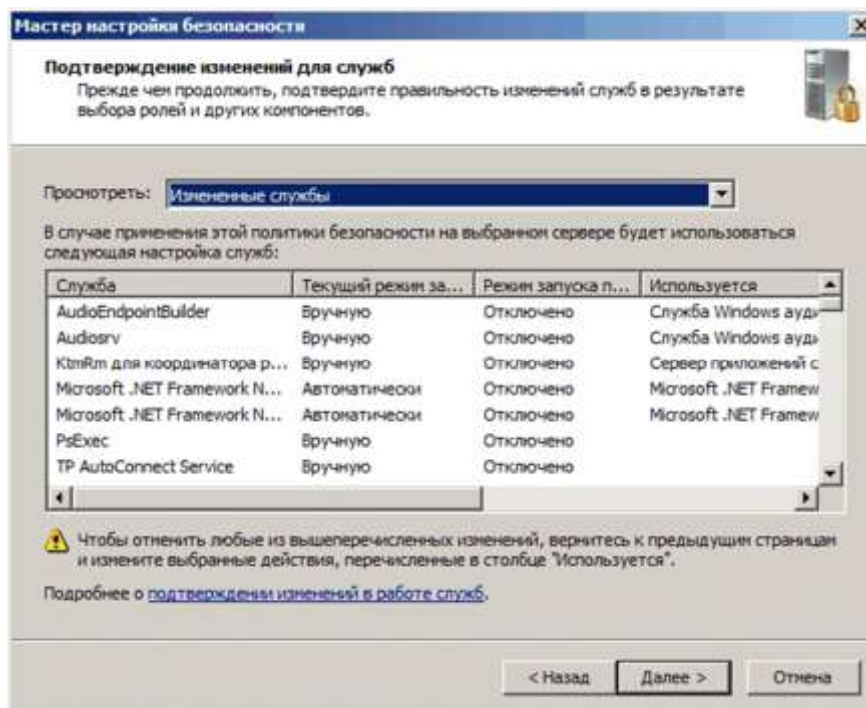
Службы, найденные *SCW* на компьютере и отсутствующие в базе данных, показываются на странице дополнительных служб. Поскольку все встроенные службы должны быть описаны в базе, этот диалог обычно возникает, если установлены какие-либо службы от сторонних производителей.



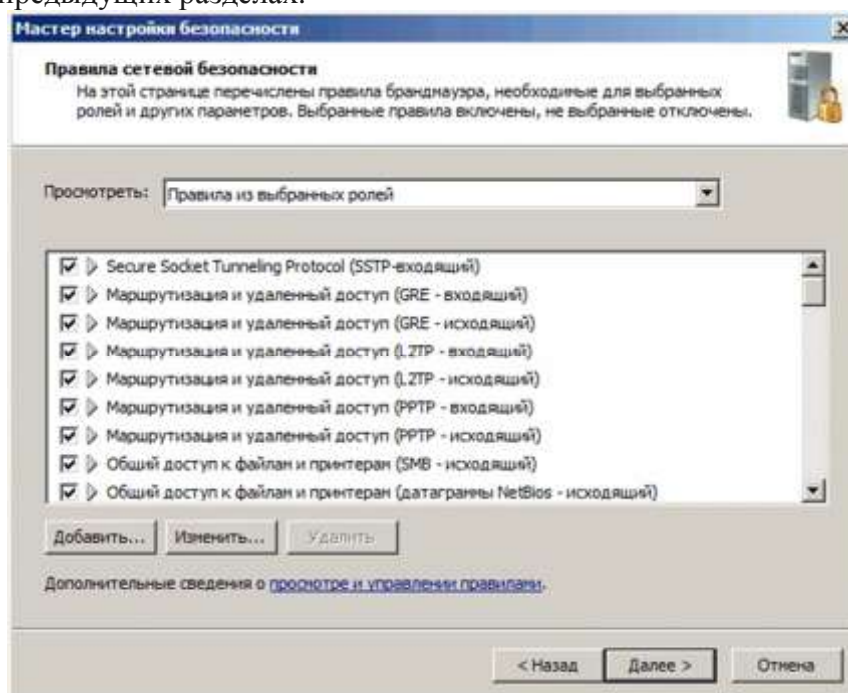
Затем мастер предлагает выбрать, что делать со службами, которые на данный момент не определены. Этот вариант предназначен для случаев, когда создаваемую политику предполагается применить к другому компьютеру, который содержит иной набор служб, чем тот, на котором создается политика. По умолчанию предлагается оставить их в покое. Второй вариант – отключить их, это более безопасно, но может вызвать сбои в работе сервера.



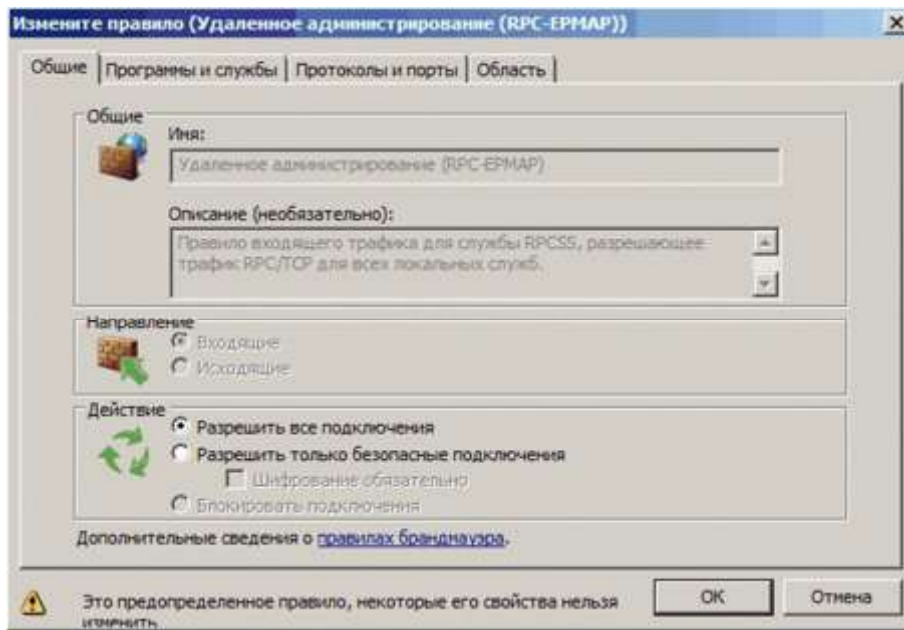
Завершая работу с разделом настройки ролей, подытожим сделанное. Как мы видим, SCW отключает все службы, которые не нужны для выполнения сервером своих задач, тем самым уменьшая область, доступную для атак.



Следующий этап *SCW* — настройка правил сетевой безопасности. После первоначальной страницы приветствия появляется диалог правил сетевой безопасности. Здесь нам предлагается список всех правил брандмауэра, основанных на поддержке ролей, выбранных в предыдущих разделах.

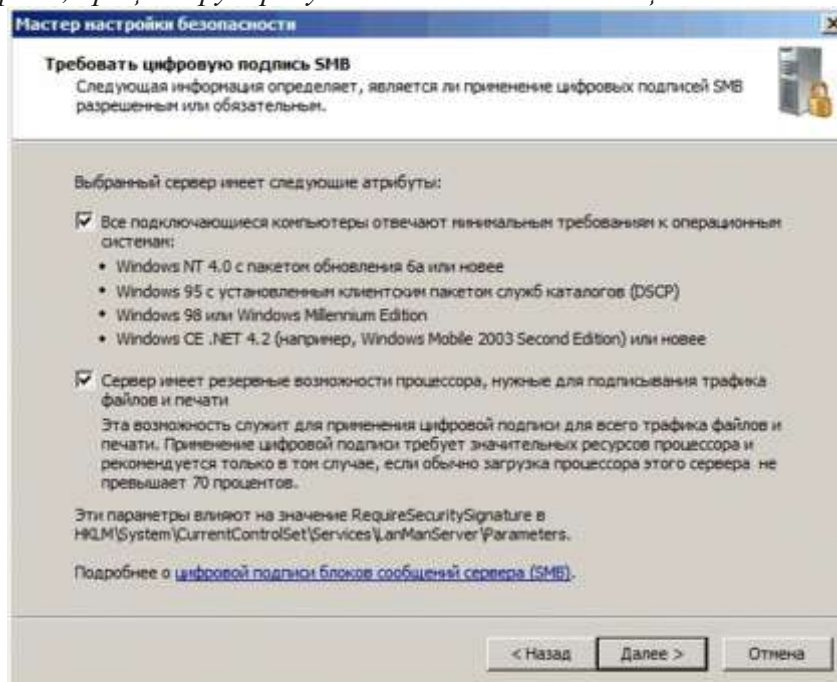


Можно не производить настроек в разделе работы с сетью, тогда *SCW* создаст правила брандмауэра, блокирующие сетевые интерфейсы так, что будут доступны только выбранные роли и компоненты. А можно усилить безопасность сервера, дополнительно настроив предложенные правила. Для этого выбираем правило и нажимаем кнопку «Изменить». Здесь можно затребовать проверку подлинности *IPsec*, включить шифрование, а на вкладке «Область» можно ограничить подключение только с определенных *IP*-адресов.

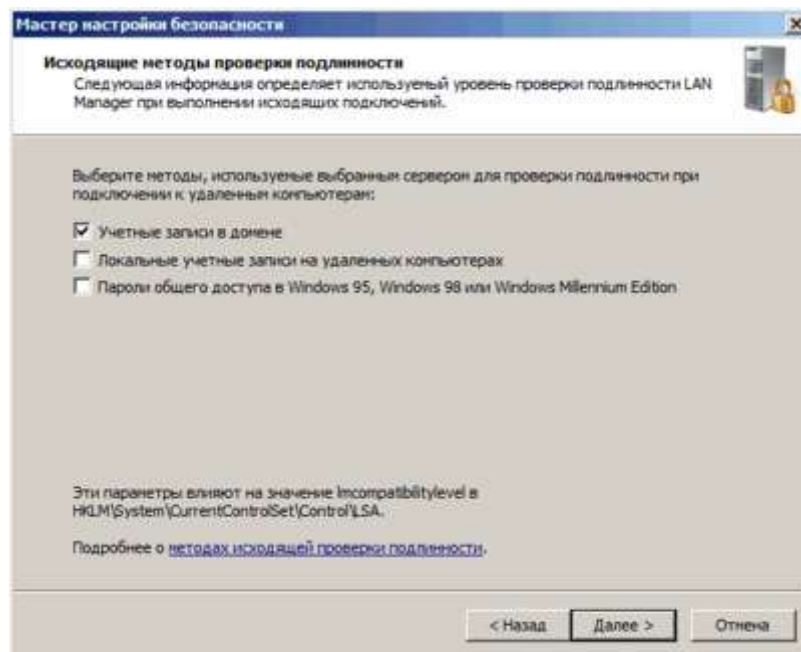


Следующий, третий раздел — параметры реестра. В нем мы вносим изменения в настройки реестра, отвечающие за связь с другими компьютерами — протоколы, типы аутентификации и т.п. Это может потребоваться для блокировки обмена данными с определенным типом клиентов, например работающих под управлением более ранних версий Windows. Также, при наличии свободных мощностей процессора можно включить подписывание трафика, передаваемого по протоколу SMB.

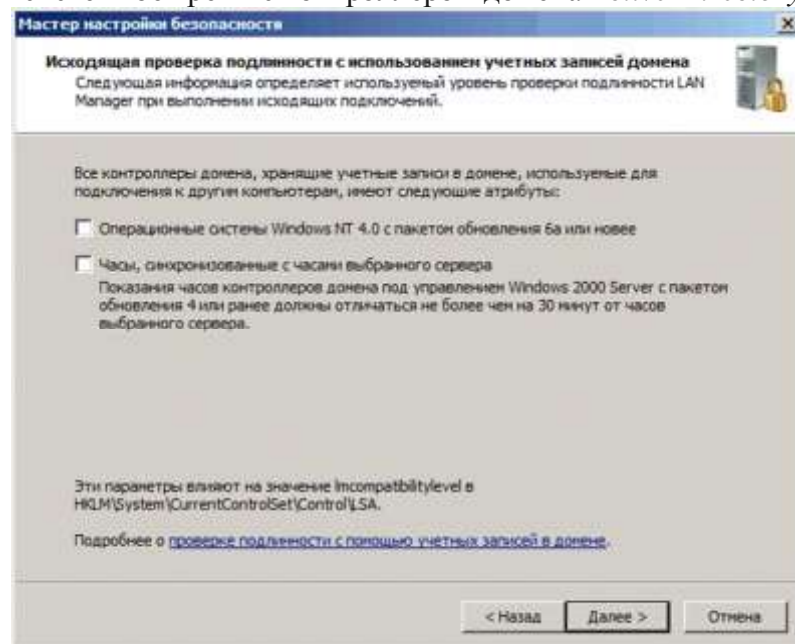
Подписывание SMB осуществляет проверку подлинности, помещая цифровую подпись в каждый блок сообщений SMB. Затем цифровая подпись проверяется как клиентом, так и сервером. За преимущества подписывания SMB приходится расплачиваться быстродействием. Несмотря на то, что работа протокола не требует затрат сетевого трафика, процессору требуются дополнительные циклы для подписывания.



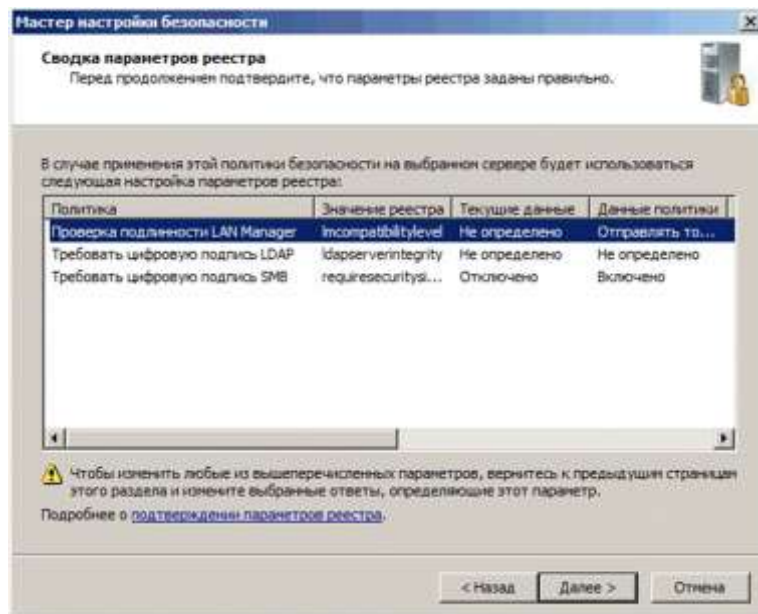
Затем следует выбор метода проверки подлинности (аутентификации) при подключении к удаленным компьютерам. Если сервер является членом домена, то однозначно выбираем доменные учетные записи, если нет — то локальные.



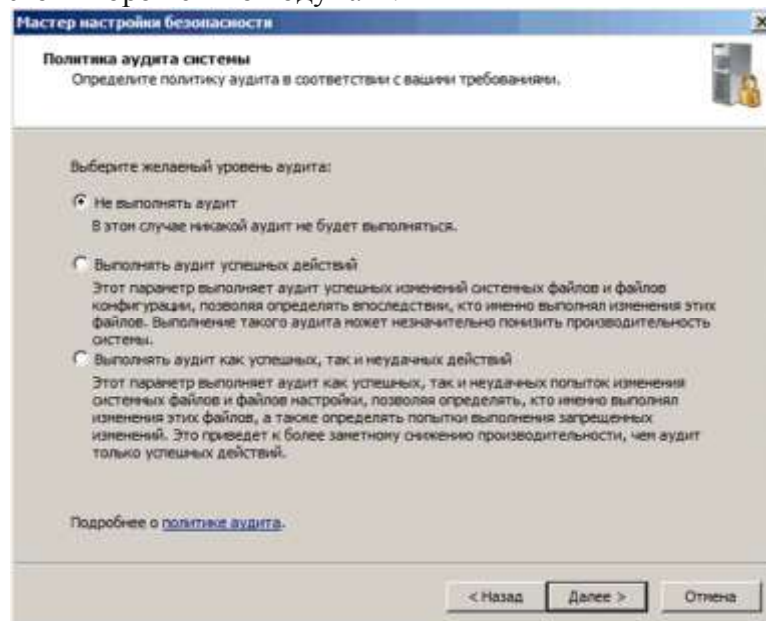
Если выбрана доменная аутентификация, то здесь можем ограничить общение нашего сервера с системами не ниже *Windows NT 4.0 SP6A* (если такие еще остались). А если клиенты должны синхронизировать свои системы именно с этим сервером, мы также можем выбрать эту опцию здесь, хотя по умолчанию большинство систем синхронизируют системное время с контроллером домена *Active Directory*.



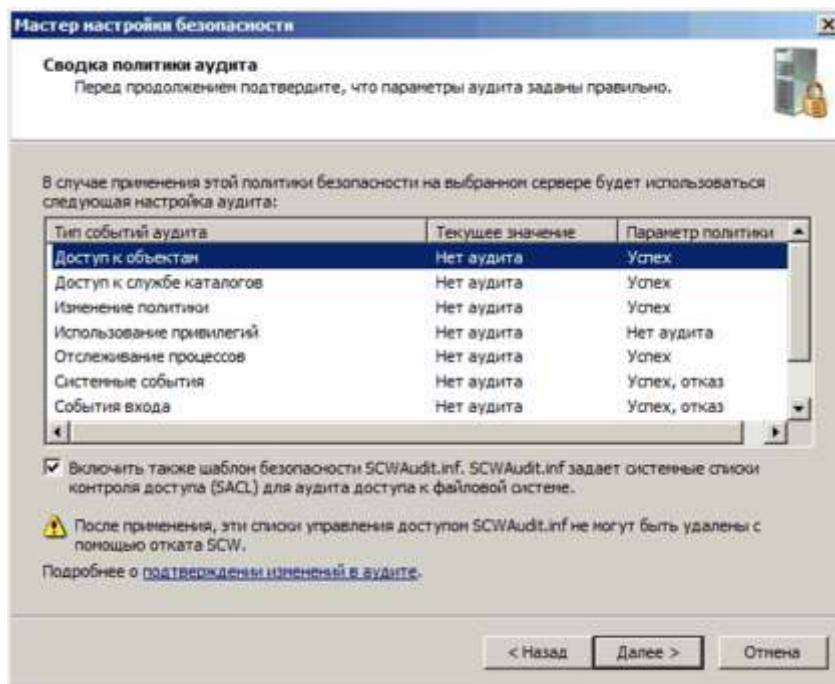
И в завершение смотрим изменения в реестре.



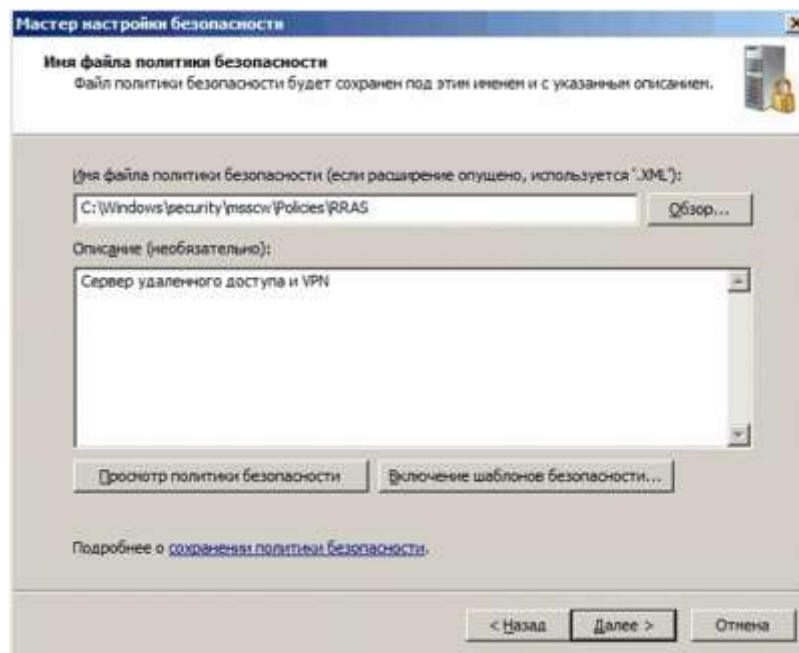
Последний раздел — настройка политик аудита. В зависимости от требуемого уровня безопасности можно не включать аудит вообще, включить только аудит успешных действий или аудит всех действий на сервере. Имейте в виду, что аудит требует немало системных ресурсов, да и на чтение журналов безопасности придется потратить немало времени, так что стоит хорошенько подумать.



Затем смотрим изменения, внесенные в политику аудита. Обратите внимание на то, что опция, включающая шаблон безопасности *SCWaudit.inf* по умолчанию включена. Этот шаблон служит для упрощения аудита доступа к файловой системе. Будьте осторожны — когда шаблон *SCWaudit.inf* применен, его нельзя удалить с помощью функции отката в *SCW*.



На этом этапе настройки завершены. Остается только сохранить созданную политику. Для этого нужно указать место для сохранения файла политики и добавить ее описание. Также можно просмотреть политику или подключить дополнительные шаблоны безопасности.



В завершение мастер предлагает нам выбрать, применить сразу созданную политику или отложить решение этого вопроса. Отмечаем нужный вариант, жмем кнопку «Далее», затем «Готово». На этом работа мастера завершена.



Также следует упомянуть об утилите командной строки **scwcmd.exe**, при помощи которой можно производить некоторые действия с созданными политиками:

- **scwcmd view /x:<Policyfile.xml>** — просмотр созданной политики;
- **scwcmd configure /p:<Policyfile.xml>** — применение созданной политики;
- **scwcmd rollback** — откат последней примененной политики;
- **scwcmd transform /p:<Policyfile.xml> /g:<GPODisplayName>** — преобразование политики в объект групповой политики (*GPO*).

Полный набор возможностей утилиты можно посмотреть командой **scwcmd /?**

После завершения работы мастера сдать преподавателю выполненную работу.

Список источников

1. Операционные системы, среды и оболочки: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013.
2. Операционные системы. Основы UNIX: Учебное пособие/ВавренюкА.Б., КурьшеваО.К., КутеповС.В. и др. - М.: НИЦ ИНФРА-М, 2015
3. Компьютерные сети: Учебное пособие / А.В. Кузин. - 3-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014.

Заключение

Данное пособие разработано в соответствии с рабочей программой ПМ.02 Обеспечение информационной безопасности для студентов техникума.

Приобретенные студентами практические навыки практической работы позволяют более глубоко усвоить основные понятия и принципы настройки и администрирования компьютерных систем..

Кроме того, практическая деятельность делает занятия увлекательными и прививает навыки работы с электронной средой и оборудованием, развивает наблюдательность и умение логически мыслить.

После проведения данного практикума студенты должны:

- уметь производить настройку оборудования и программного обеспечения;
- отработать на практическом опыте алгоритмы настройки оборудования;
- подтверждать практическую значимость работы теоретическим материалом.