KAK - AD RMS

Часть 1 – развертывание

Несмотря на то, что служба AD RMS в Windows 2008 R2 является уже четвертым выпуском службы управления правами, она по-прежнему остается «редким зверем» в зоопарке ИТ-решений российских системных администраторов. Ответить на вопрос, почему так сложилось, довольно сложно, возможно, отчасти из-за недопонимания сути технологии и некоторых требований к уже имеющейся инфраструктуре, отчасти из-за ее несколько показушной защиты. Я не буду пытаться хвалить или наоборот выливать ушат грязи на AD RMS, а попытаюсь провести некий экскурс по ее настройке и администрированию, дабы читатель сам смог решить вопрос о необходимости подобного решения.

Отличие AD RMS от других средств защиты данных

Согласно модели защиты «**Defense-in-Depth**»на каждом из 7 уровней действуют свои средства обеспечения безопасности и если начать их перечислять, то станет понятно, подавляющее их большинство препятствует получению злоумышленником доступа к данным компании. И только лишь шифрование остается последнее преградой, когда информация находится в руках у злоумышленника. Задача AD RMS –сохранить конфиденциальность данных, при этом добавив гибкости и свободы в их распространении.

Пример из жизни.Вы хотите опубликовать в рамках своего департамента эл. документ,распространение будет осуществляться самыми различными способами (эл. почта,копирование по сети, CD, Flash-носители). При всем этом у вас есть строгое требование: ограничить круг читателей документа сотрудниками вашего департамента, а также быть уверенным в том, что документ не будет модифицирован или распечатан. Это задача вполне под силу AD RMS.

Вывод. AD RMScоздан для обеспечения конфиденциальности документов независимо от способа хранения и распространения. Документы, защищенные AD RMS, шифруются, а автор может устанавливать разрешения для тех, кто получит доступ к данным.

Список возможных ограничений прав:

- Чтение, Изменение, Печать
- Срок действия документа
- Запрет пересылки электронного письма
- Запрет печати электронного письма

Клиентскими операционными системами могут выступать:

- Windows 2000
- Windows XP
- Windows 2003 /2003 R2
- Windows Vista
- Windows 7
- Windows Server 2008 /2008 R2
- Windows Mobile 6

При наличии продуктов Exchange Server 2007 SP1 и SharePoint Server 2007 после установки AD RMS появляются дополнительные средства обеспечения безопасности. В частности в SharePoint Server 2007 появится возможность защищать библиотеки документов.

Необходимые условия для внедрения.

Как я уже сказал, AD RMS выдвигает определенные требования к существующей ИТ-инфраструктуре. Для того, что бы понять, как будет выглядеть наше решение, предлагаю рассмотреть Рис.1

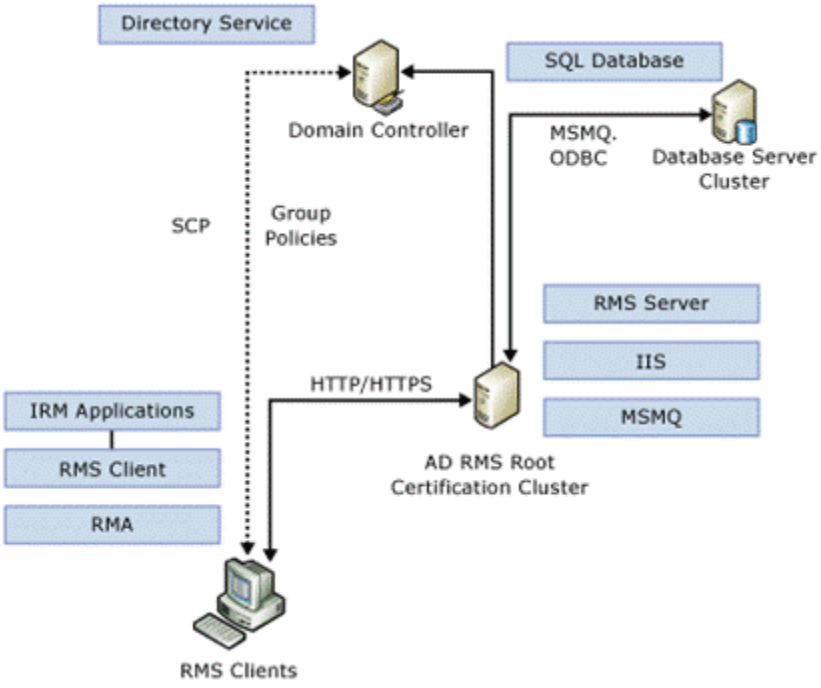


Рис. 1. Компоненты решения AD RMS

Стартовой площадкой и обязательным условием является наличие работоспособной службы **Active Directory Domain Services (AD DS)**. При этом контроллер домена обязан быть на базеWindows Server 2000 SP3 или более поздних версий ОС. AD RMS перекладывает на службу AD DS задачу аутентификации и хранит в каталоге необходимый клиентам URLгруппы AD RMS серверов. Все пользователи и группы пользователей, которые будут работать с AD RMS должны иметь адрес электронной почты, настроенный в Active Directory DS. Это необходимо для получения доступа к защищенному содержимому и самостоятельной публикации защищенных документов.

Как и большинство продуктов Microsoft AD RMS требует наличия сервера баз данных, а именно SQL-сервера. Поскольку мы говорим об AD RMS на платформе Windows Server 2008 R2, то следует учесть отсутствие поддержкиMicrosoft SQL Server 2000. Поэтому в качестве SQL-сервера следует использовать версии **Microsoft SQL 2005/2008**. При отсутствии SQL допускается использование внутренней базы Windows (Windows Internal Database), что сразу накладывает ограничение в использовании только одного сервера AD RMS.

Клиентами могут выступать операционные системы Windows 2000, Windows XP и Windows 2003; при этом для работы с AD RMS на них будет необходимо установить клиентскую часть (AD RMS Client), скачиваемую с сайта Microsoft. С выходом Windows Vista SP1 и Windows 7 ситуация несколько упростилась, теперь клиент RMS интегрирован и дополнительной установки не требует. С версиямиMicrosoft Office также есть определенный нюанс, так **Office 2007 Ultimate, Professional Plus, Enterprise** дают возможность как защищать документы, так и пользоваться защищенными. В то время как более дешевые выпуски допускают только работу с уже защищенными файлами.

Ну и наконец, сам AD RMS сервер. С появлением Windows Server 2008/2008 R2 служба управления правами изменила имя и стала компонентом операционной системы, устанавливаемым как роль сервера. Эта роль отвечает за предоставление лицензий контроля доступа к содержимому. При установке первогоAD RMS сервера, создается корневой кластер AD RMS. Для повышения отказоустойчивости и доступности впоследствии возможно добавить к корневому кластеру дополнительные AD RMS сервера. Важно понимать, что в лесу Active Directory может существовать только один корневой кластер AD RMS и несколько дополнительных AD RMS серверов лицензирования. Фактически AD RMS licensing-onlyсервер представляет собой филиальное решение, которое может быть развернуто для увеличения производительности и понижения использования WAN-канала в случае нахождения клиентов и AD RMS кластера в разных сайтах.

Развертывание

Самый просто способ понять AD RMS и разобраться в его работе– это настроить самостоятельно тестовый стенд. Развертывание я буду производить в виртуальной среде, состоящей из двух серверов: Server1 и Server2.

Server1.

ОС: Windows 2008 R2

Является контроллером домена (itband.ru) в лесу Active Directory уровня Windows 2008 R2. Сетевой интерфейс сконфигурирован следующим образом: IP – 192.168.0.1; Маска подсети: 255.255.255.0; DNS – 192.168.0.1. Для тех, кто испытывает трудности с настройкой службы AD DS, я записал видео-демонстрацию. Скачать Видео «Поднятие первого контроллера домена в лесу (Server1)» можно по этой ссылке.

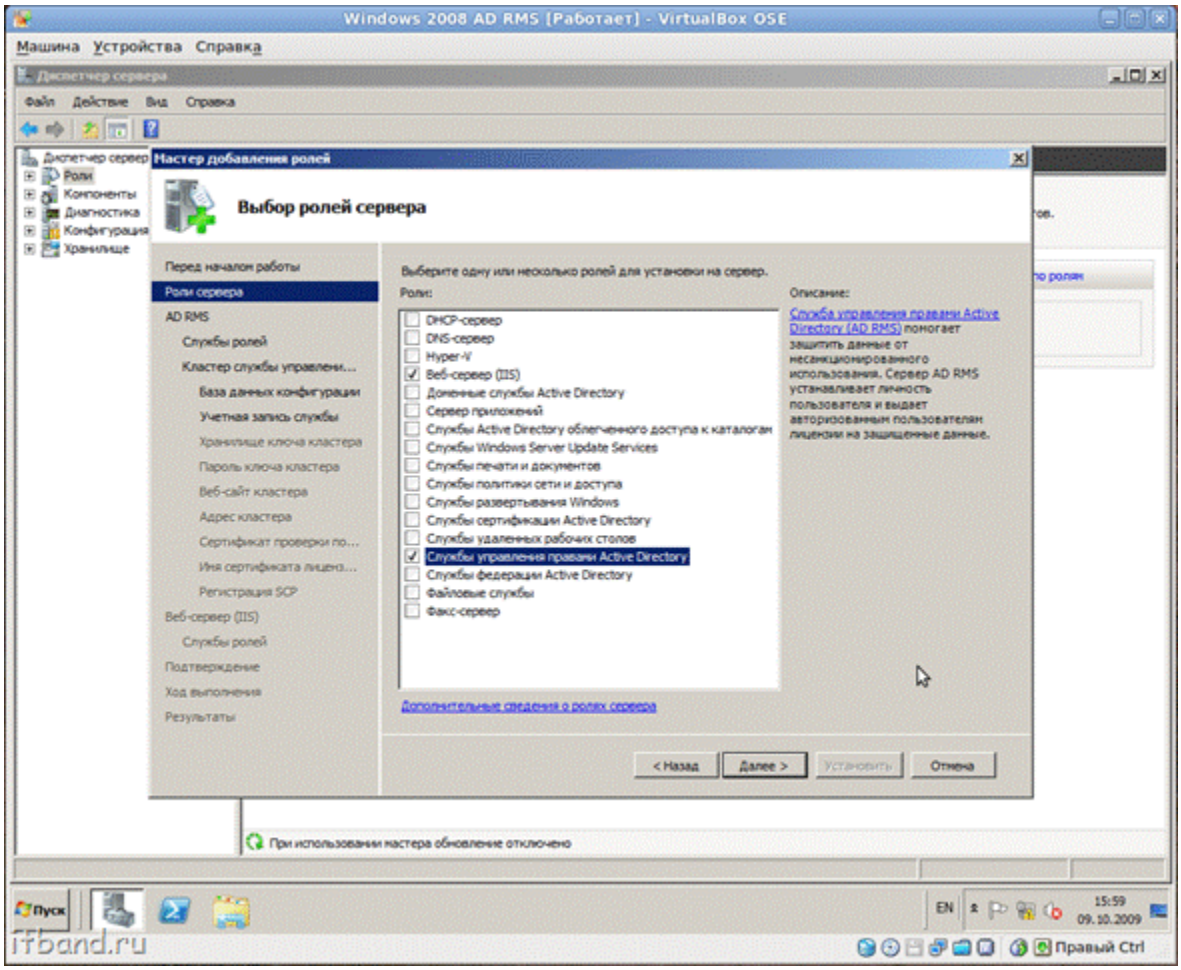
Поскольку AD RMS требует для работы SQL-сервер и при настройке создает две базы данных (**Configuration Databaseи Logging Database**) мы установим его (SQL) на Server1. При настройке я использовал SQL Server 2008 Standart x64; сразу замечу, что из всего многообразия компонент SQL для AD RMSнужны компоненты **Database Engine** и полный набор **Средств Управления**.После инсталляции SQL Server 2008 в обязательном порядке требуется установка пакета обновления SP1, который добавляет совместимости с Windows 2008 R2.Читателям, не имеющим опыта инсталляций SQL Server 2008, будет интересно видео«Установка SQL Server 2008 на Server1», которое скачивается по ссылке.

Server2.

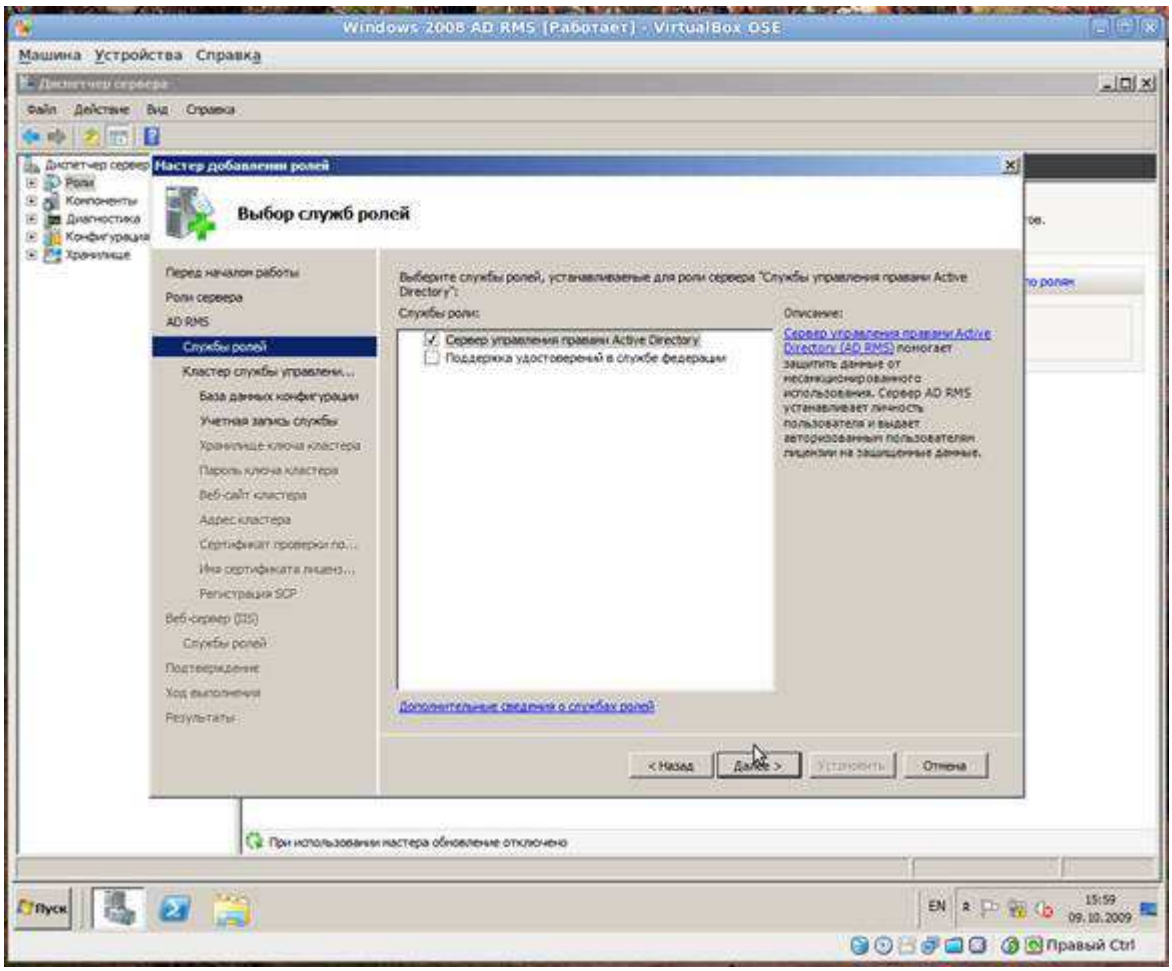
ОС: Windows 2008 R2

Данный сервер нам и предстоит настроить, установив на нем службу управления правами Active Directory. Сервер является членом доменаitband.ru, со следующей конфигурацией сети: IP – 192.168.0.2; Маска подсети:255.255.255.0; DNS – 192.168.0.1.

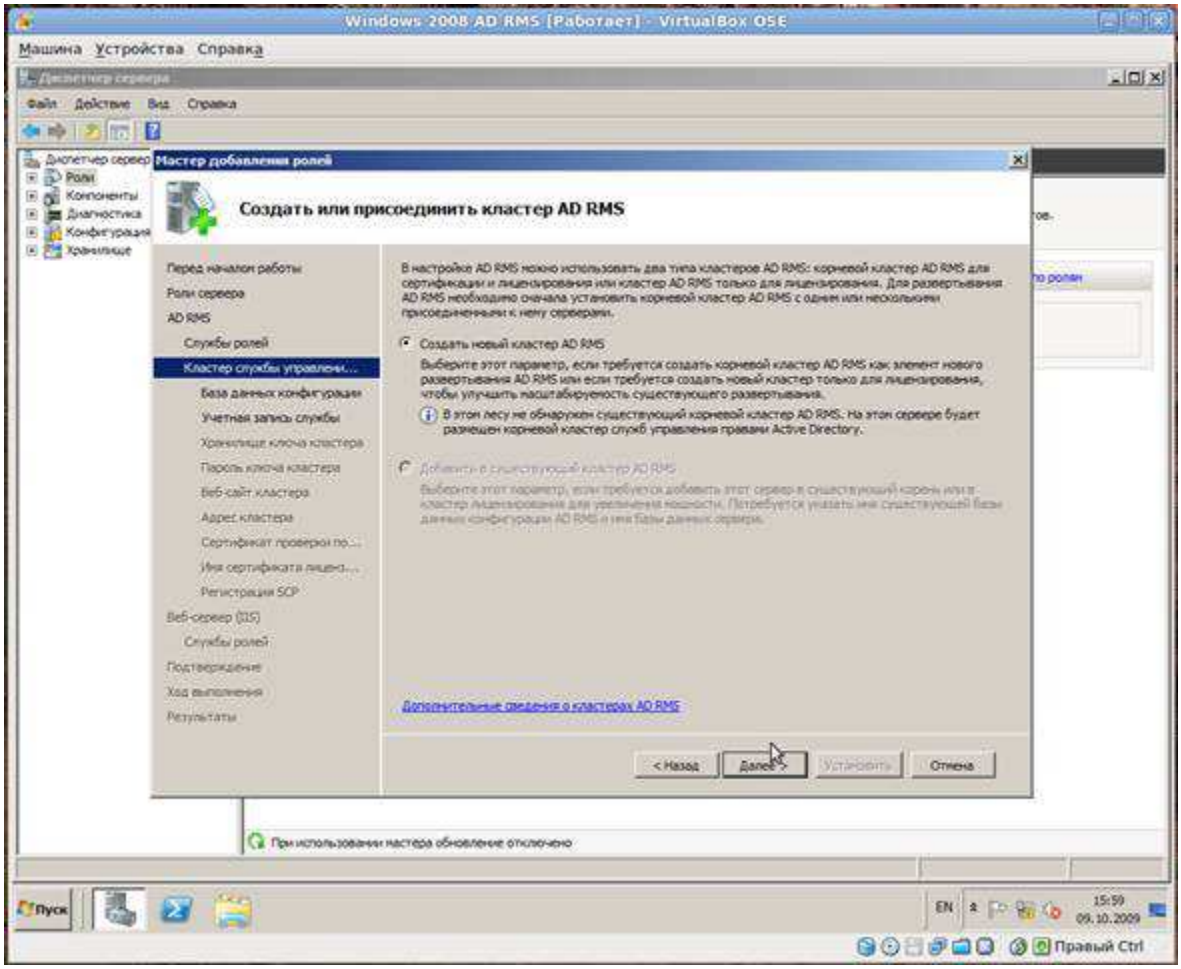
Запускаем «Диспетчер сервера» и открываем добавление новых ролей.



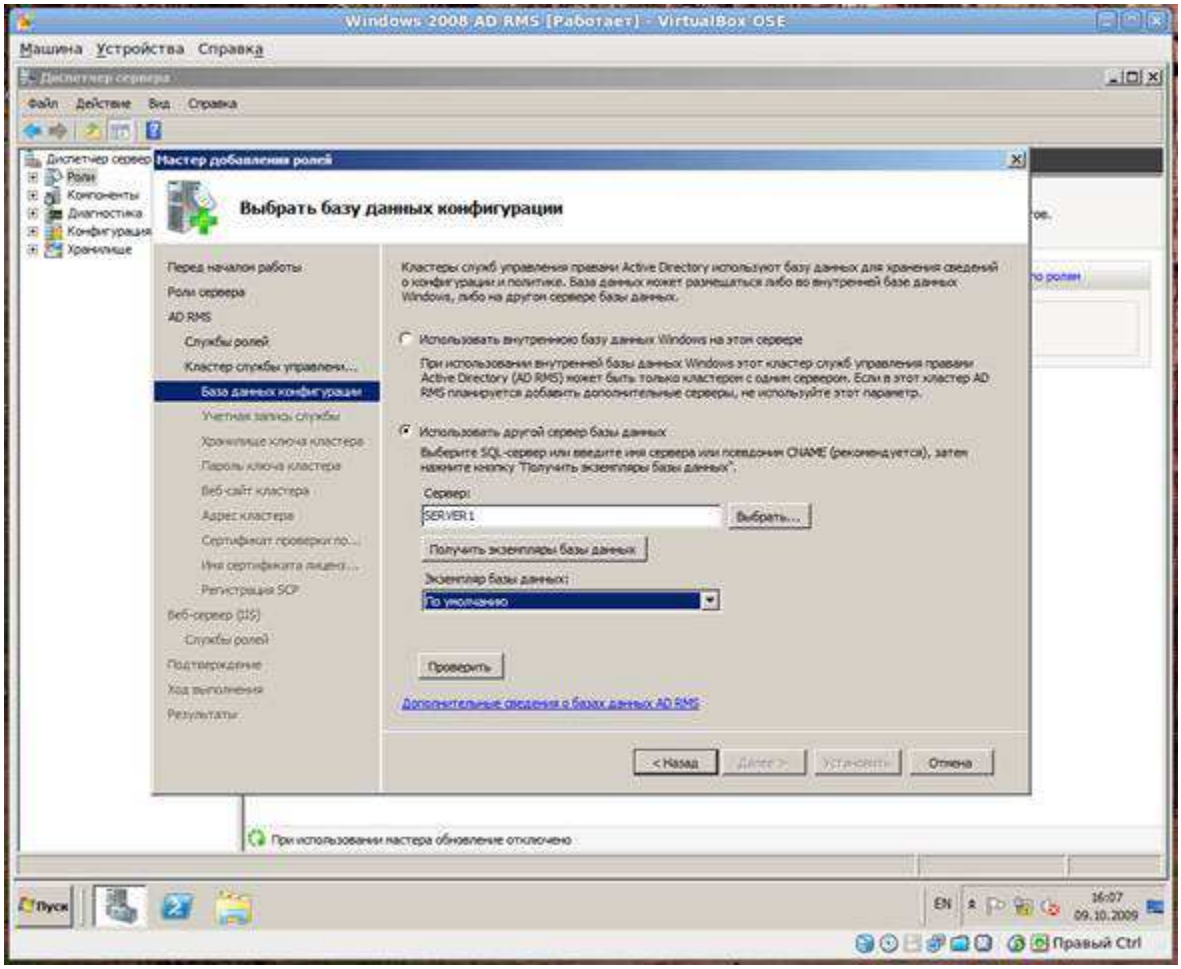
Прошу заметить, что AD RMS создает веб-сервис, и поэтому на нашем сервере должен быть установлен веб-сервер IIS с включенным ASP.NET;впрочем, добавление IIS производится автоматически при запуске установки AD RMS.



Служба AD RMS состоит из двух компонентов «Сервер управления правами Active Directory» и «Поддержка удостоверений в службе федераций».Нас интересует первый компонент. «Поддержка удостоверений в службе федераций»требуется в случае развертывания AD RMS в среде, состоящей из нескольких независимых компаний. Мы же создаем решение, которое будет использоваться только нашими сотрудниками, поэтому данную опцию опускаем.

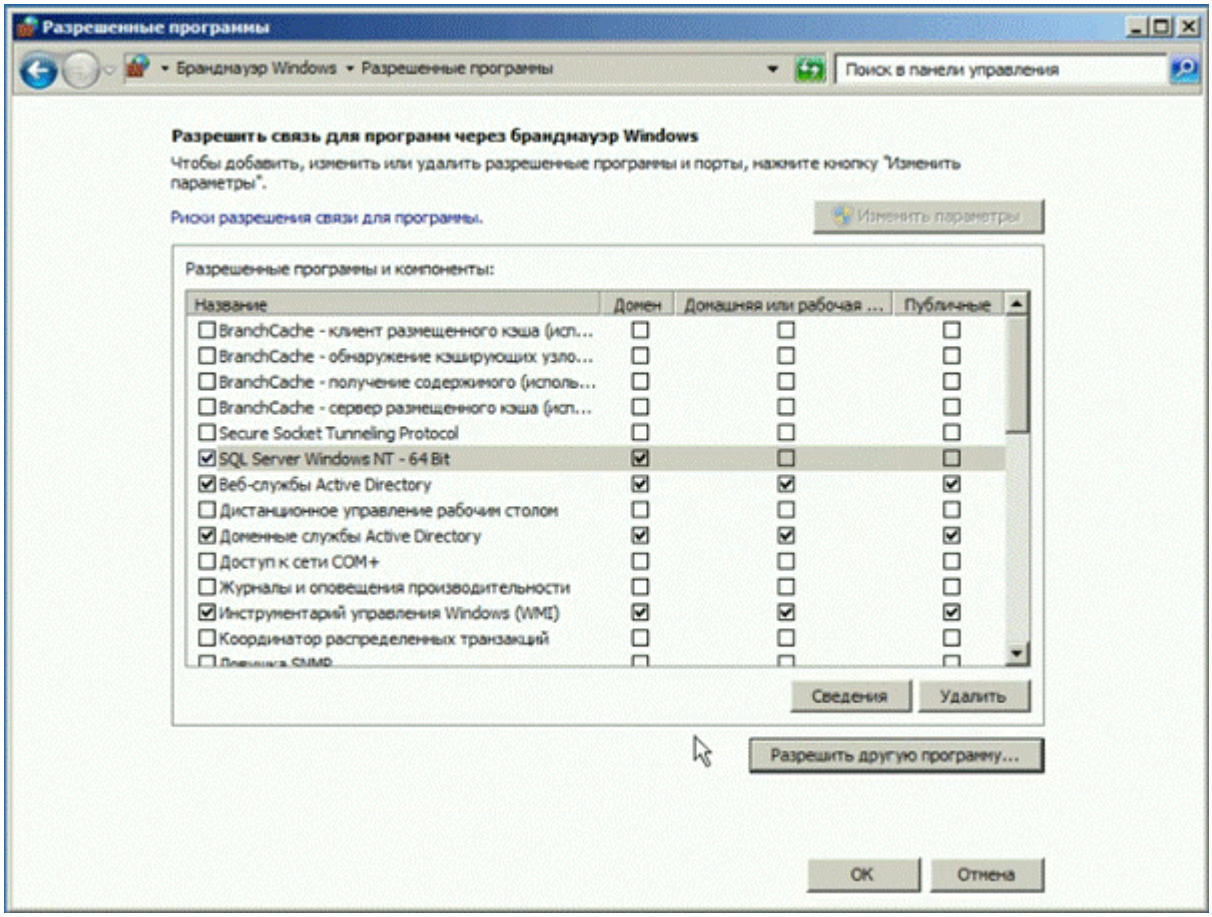


Дальше все просто, мастер спрашивает, желаем ли мы создать новый кластер AD RMS или хотим добавить сервер AD RMS в уже существующий.Поскольку это первый сервер управления правами в нашей сети, оставляем вариант «Создать новый кластер». (Другой вариант, собственно, нам выбрать и не позволено).

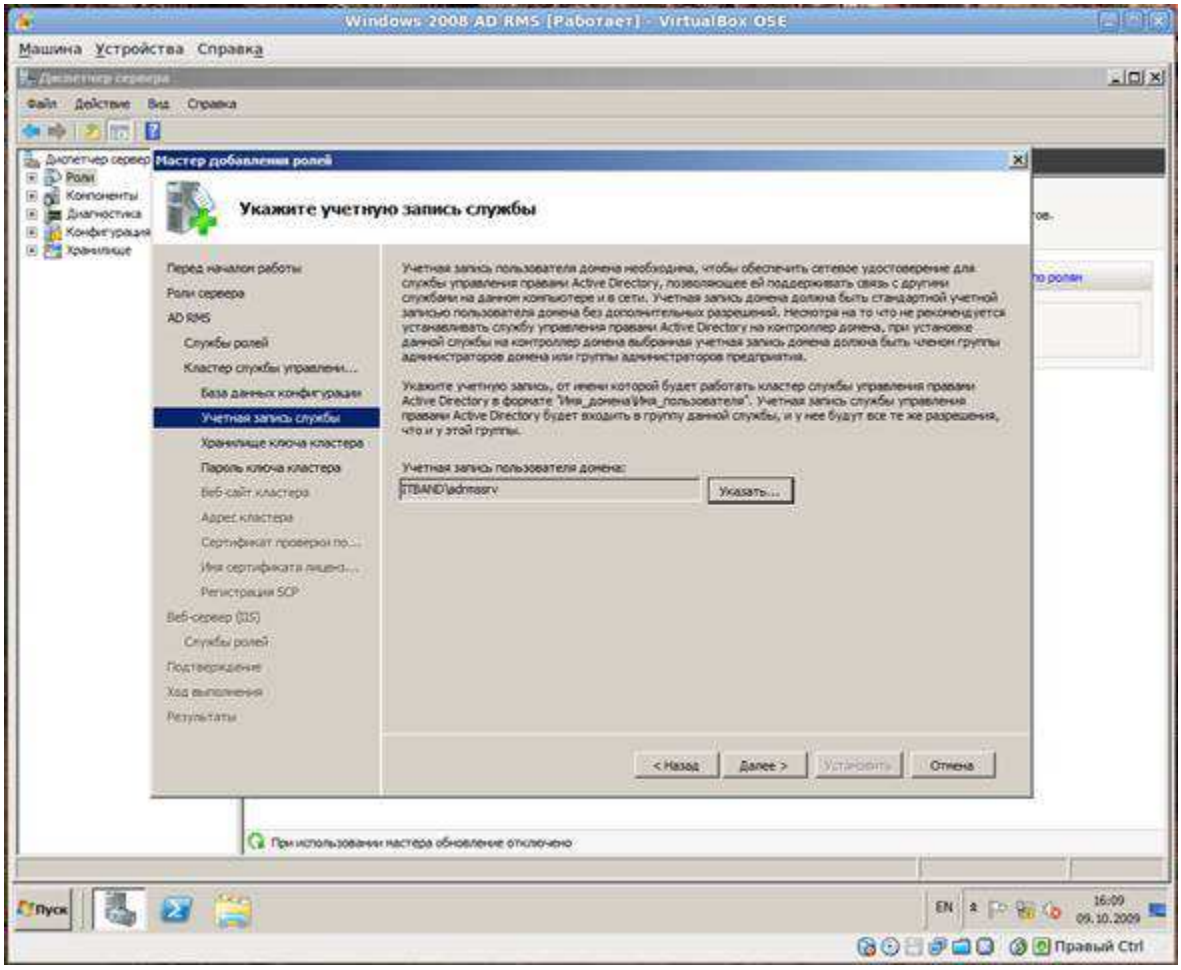


На следующем окне, мы обязаны указать место хранения базы конфигурации AD RMS и вариантов у нас несколько. Первый: «Использовать внутреннюю базу данных Windows», – с одной стороны плюс в том, чтоSQL становится не нужен, но недостаток заключается в невозможности впоследствии добавить к ферме дополнительные сервера. Поэтому, выбираем другой сервер баз данных и прописываем Server1 (а именно на нем у нас стоит SQL).

На данном этапе можно столкнуться с трудностью. При попытке получить экземпляры SQL-сервера и проверить их, сервер задумывается и сообщает о невозможности завершения операции. Все довольно просто, проблема в брандмауэре на Server1, который блокирует нужные для SQL порты. Поэтому знакомимся со статьей «Как настроить брандмауэр Windows для доступа к компоненту Database Engine»либо качаем короткое видео, где эта процедура демонстрируется.

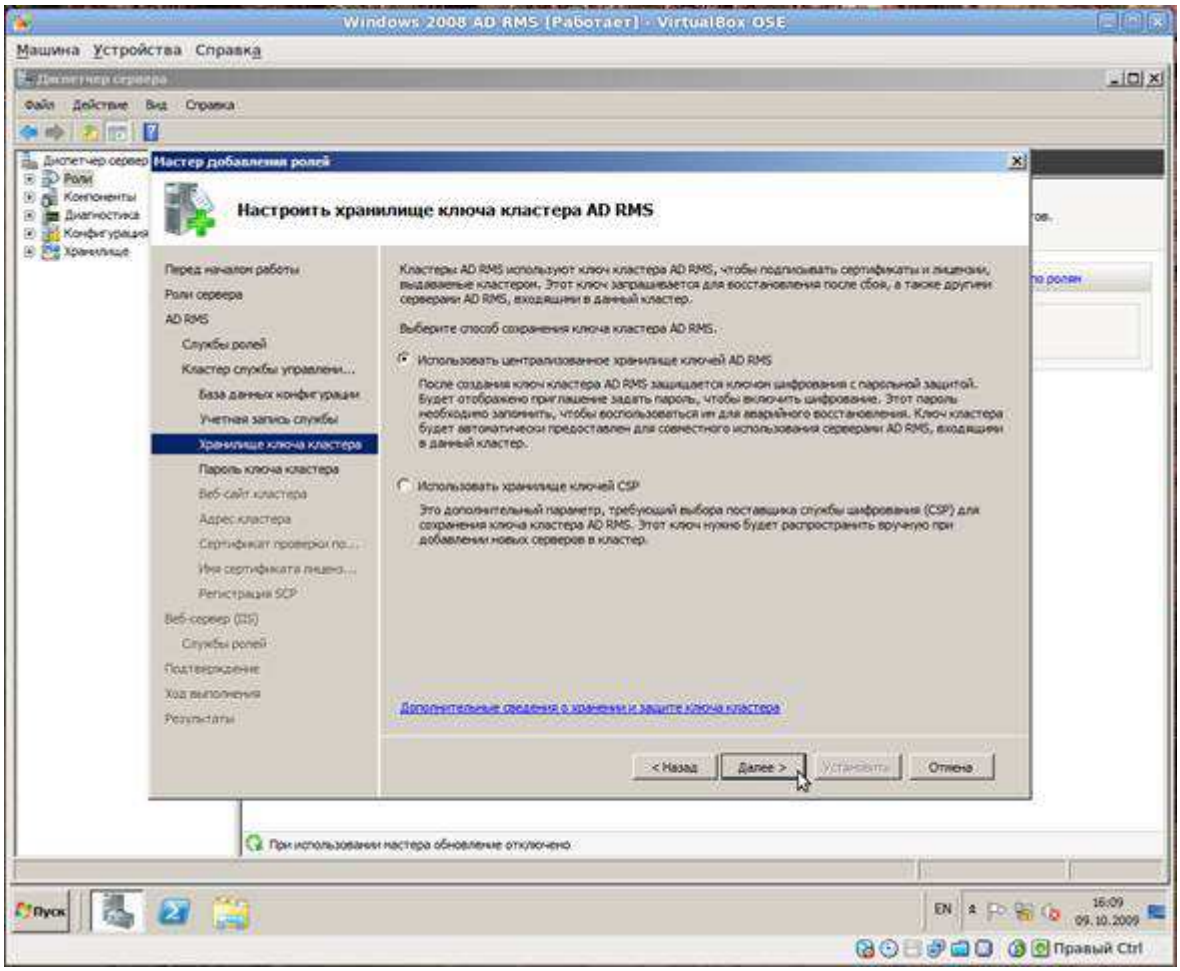


Я поступил просто и разрешил работу **Sqlservr.exe** через брандмауэр, фактически же нас интересует открытие портов 1433 и 1434.

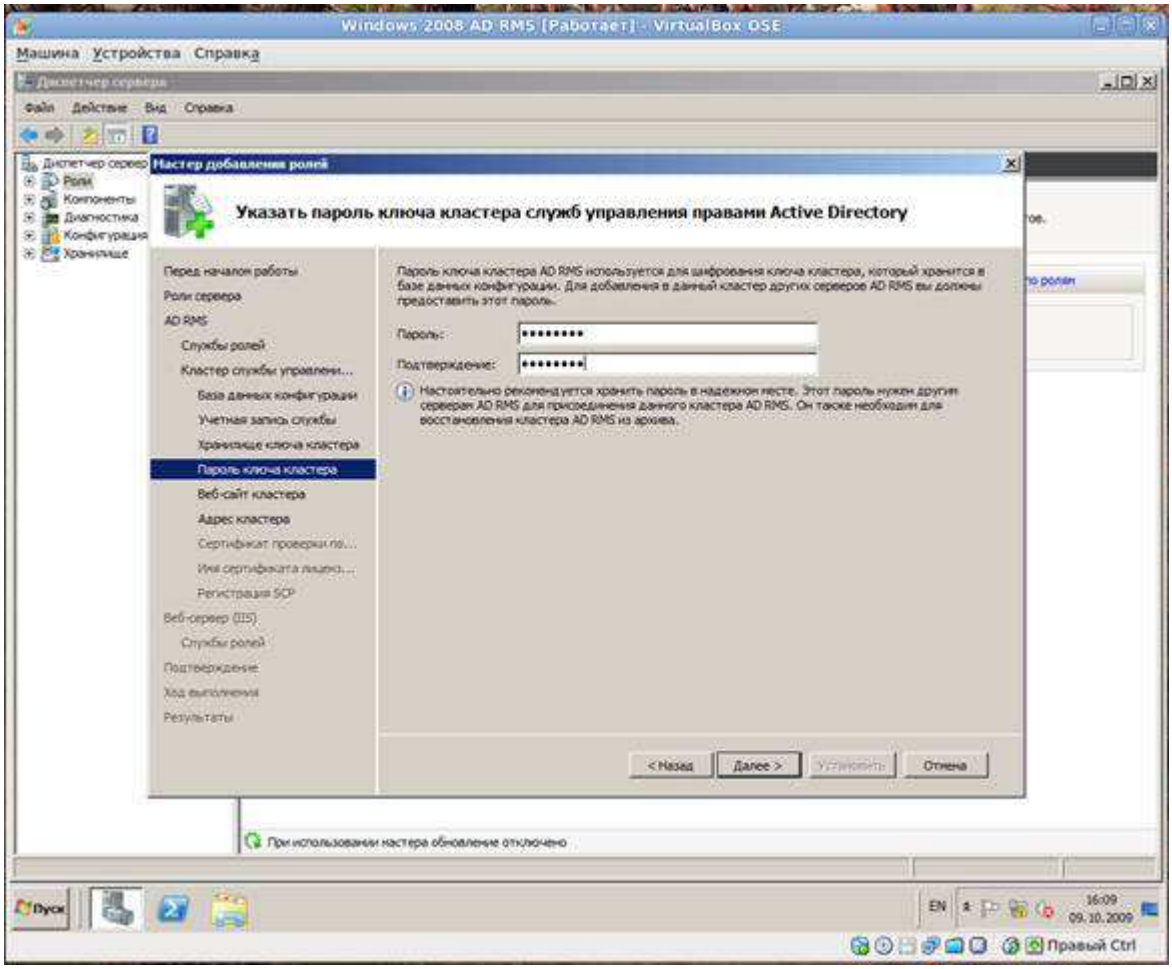


После выбора сервера баз данных, необходимо указать учетную запись, от имени которой будет работать служба управления правами.Обыкновенного доменного пользователя будет достаточно. Не забываем отключить устаревание пароля для нее и запрет смены.

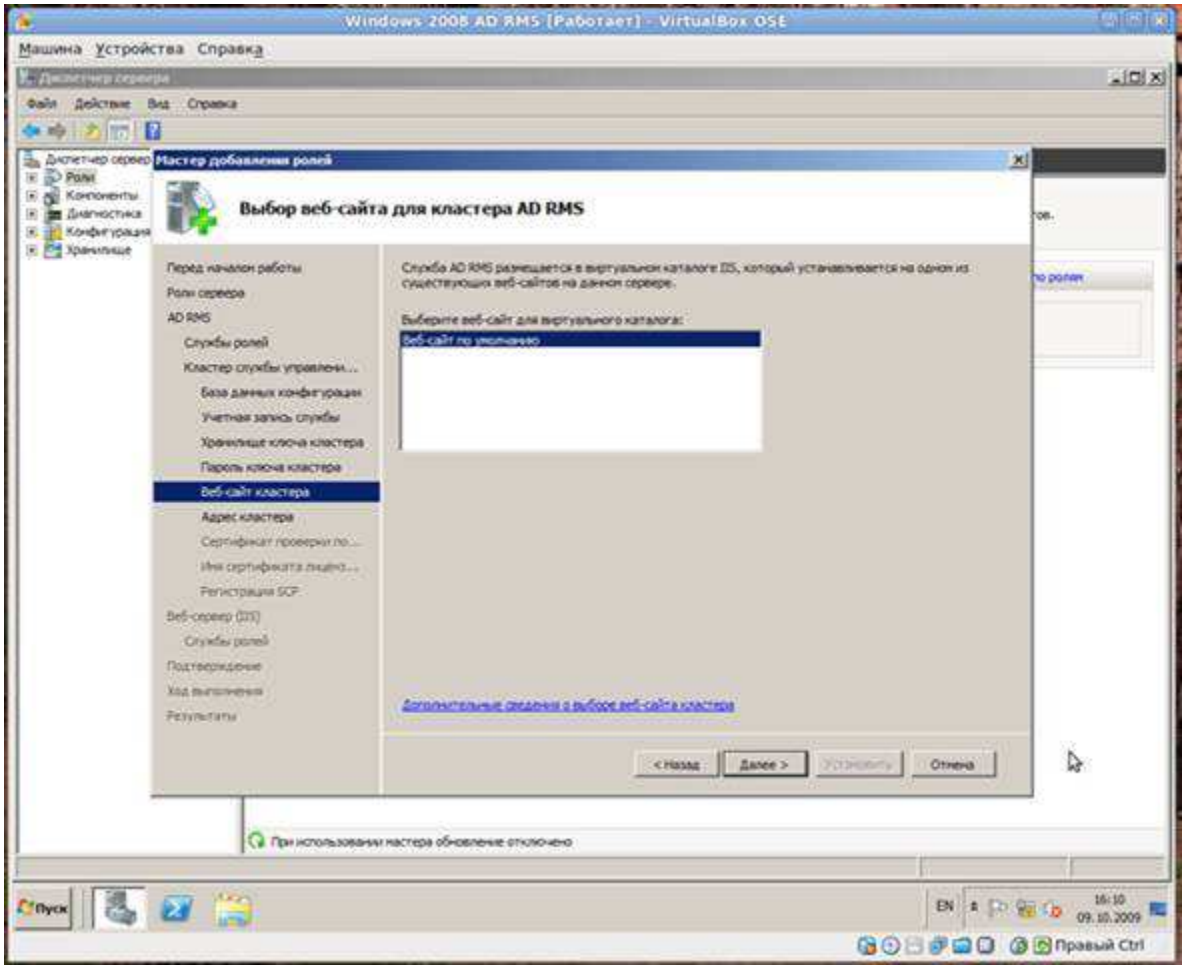
Важно. Если рольAD RMS устанавливается на контроллере домена, у учетной записи должны быть полномочия доменного администратора, что с точки зрения безопасности совсем не здорово. Поэтому такая инсталляция очень сильно расходится с «Best Practice».



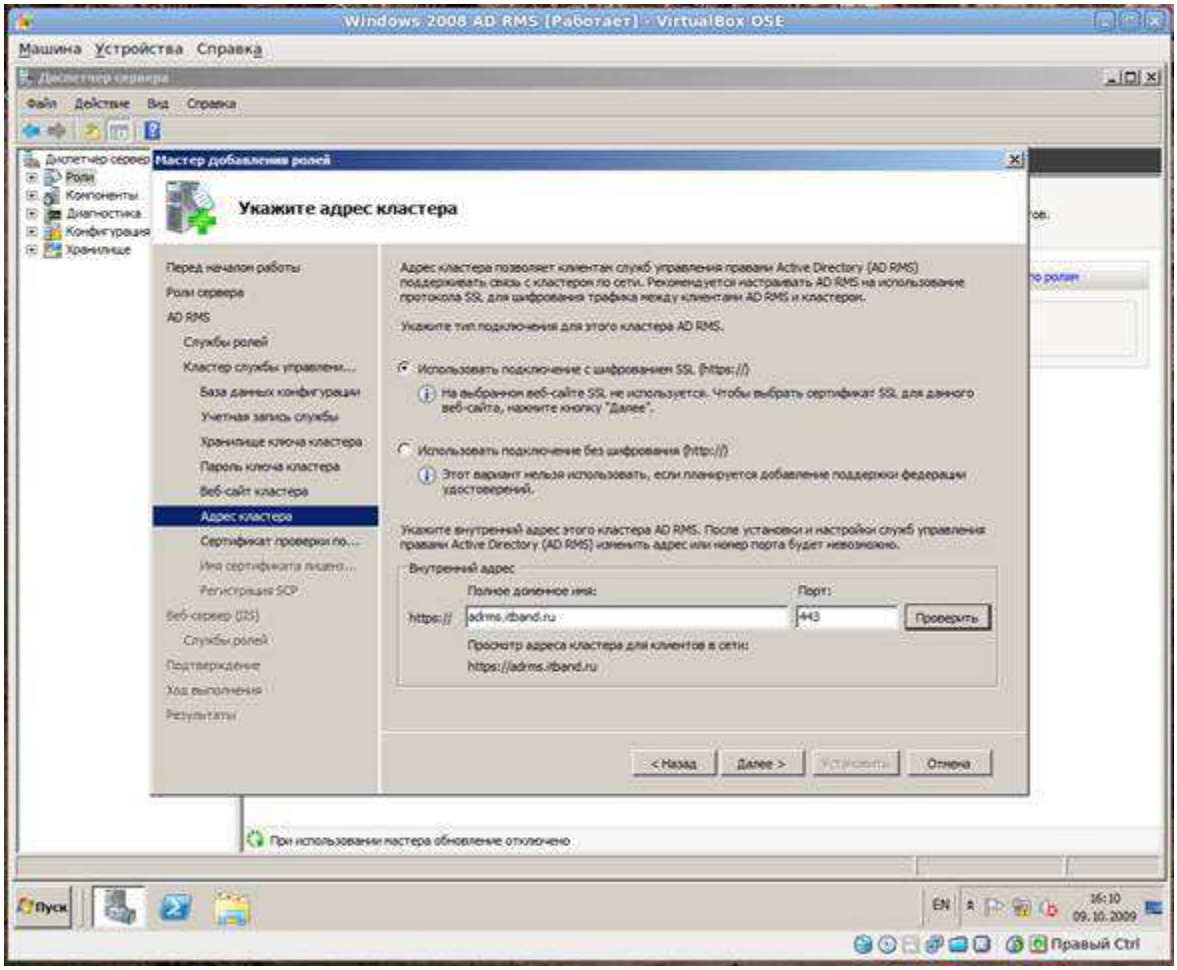
При настройке кластера создается ключ, которым будут подписываться лицензии, выдаваемые клиентам. Также ключ понадобится при добавлении нового AD RMS сервера или при восстановлении после сбоя. Возникает вопрос «Где он будет храниться?» AD RMS имеет собственное защищенное хранилище, выбор которого является предпочтительным вариантом, поскольку позволяет сделать ключ доступным всем AD RMS серверам и требует минимум участия администратора. Поэтому я остановился на варианте «Использовать централизованное хранилище ключей». В противном случае ключ сохранится в локальном защищенном хранилище и распространять его придется вручную.



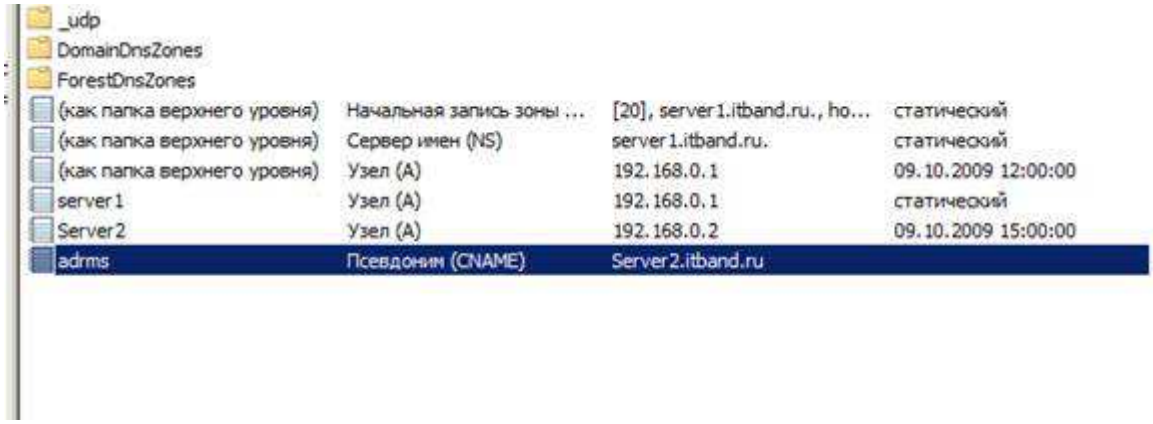
Далее задаем пароль, которым будет зашифрован ключ кластера.Пароль должен быть сложным и поступать с ним по принципу «ввел и забыл»ни в коем случае нельзя. При добавлении второго AD RMS сервера или восстановлении первого, вам придется его вспоминать.



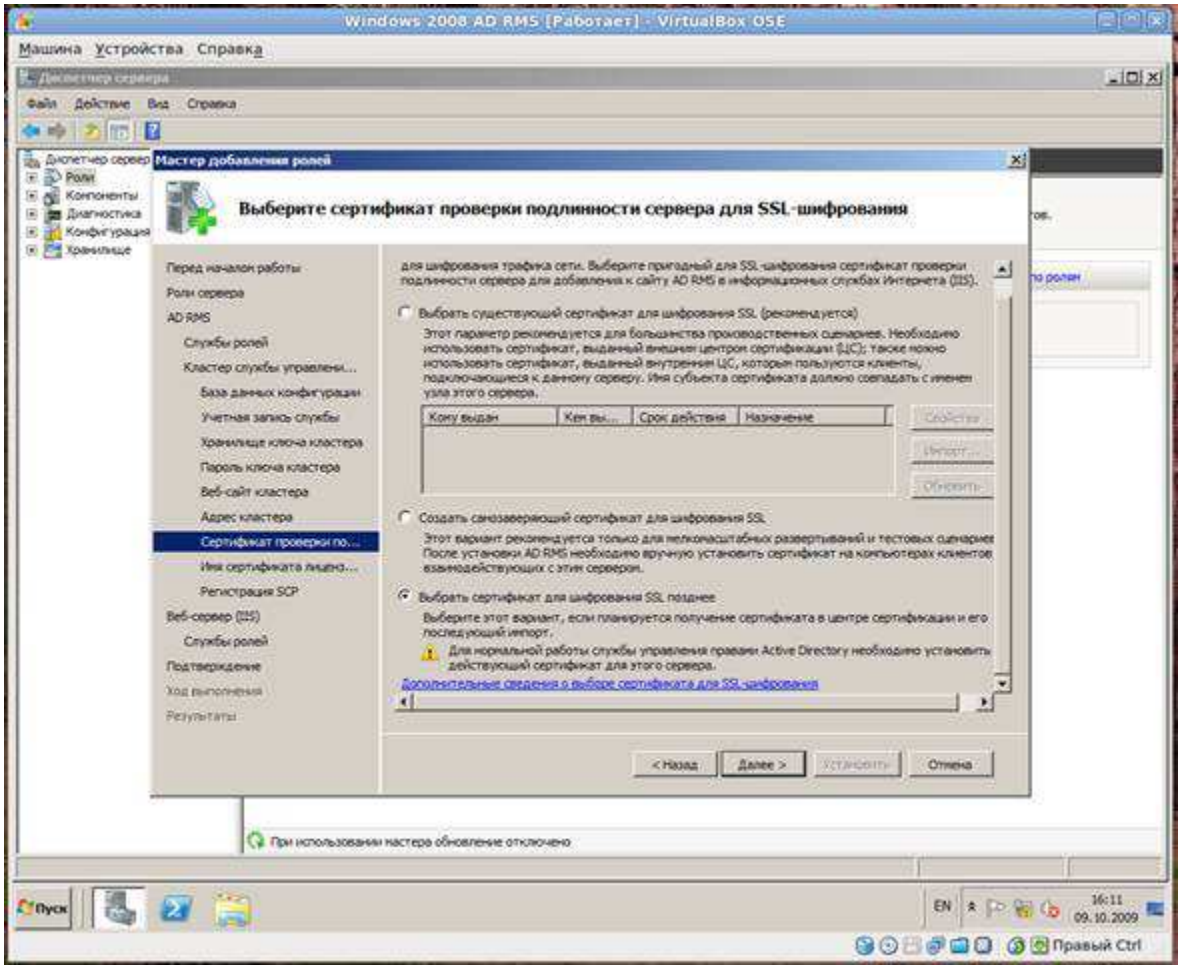
Указываем на каком веб-сайте будет запущен веб-сервис AD RMS. Я не стал изобретать велосипед и оставил веб-сайт по умолчанию.



Теперь надо указать имя и порт, по которому пользователи будут подключаться к AD RMS кластеру. Поскольку безопасность превыше всего, я выбрал SSL. Имя, по которому пользователи будут обращаться к кластеру, я задалаdrms.itband.ru, не забыв при этом создать на DNS-сервере CNAME-запись ссылающуюся на Server2.



Выбор имени и порта особенно важен, если учесть, что впоследствии эти данные будет невозможно поменять.



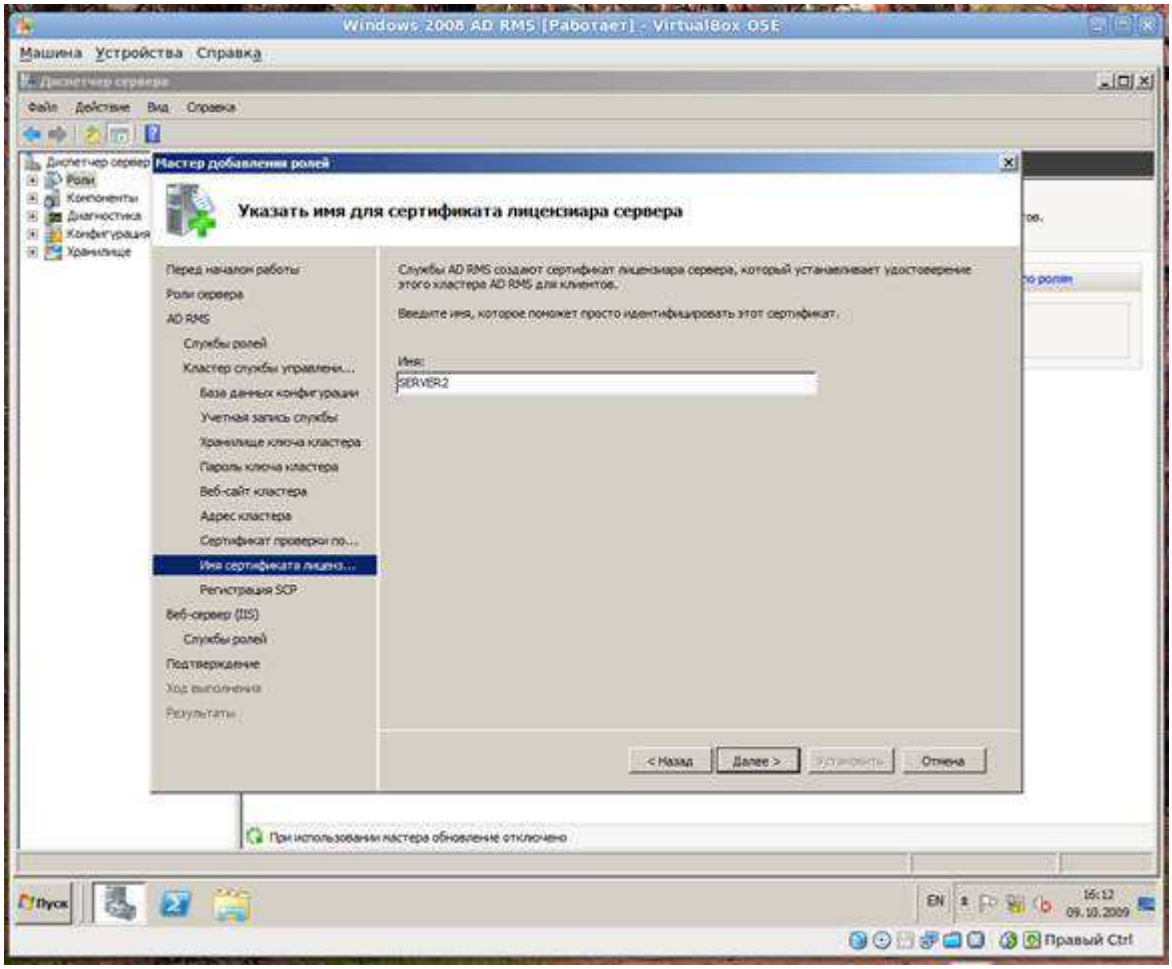
Так как на предыдущем экране мы сказали, что подключения к кластеру AD RMS будет осуществляться по протоколу https, у мастера возникает резонный вопрос «Где сертификат веб-сервера для установки безопасного канала?»

Варианты действий:

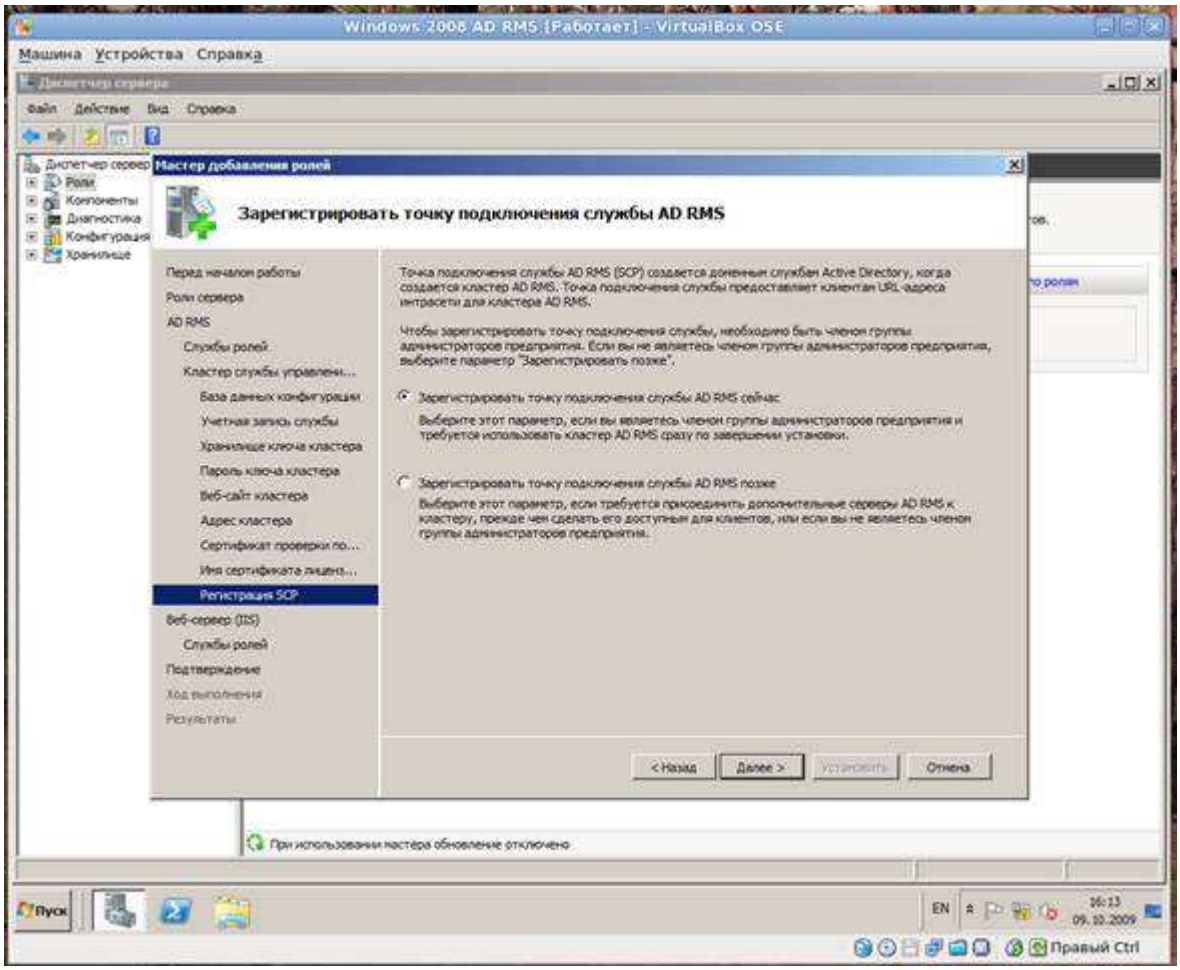
1. **Создать самоподписанный сертификат**. Самый простой путь, но к сожалению абсолютно непригодный для реальных сценариев развертывания. Ибо кроме IIS-сервера, этот сертификат придется запихивать на каждого клиента.

2. **Выбрать существующий сертификат SSL.** Т.е. каким то центром этот сертификат уже должен быть выдан. Вариантов два: купить сертификат у коммерческого CA либо настроить свой CA на базе Active Directory Certificate Services. У каждого пути свои плюсы и минусы. Моя точка зрения следующая: **если вы планируете получать доступ** к документам, защищенным AD RMS **с компьютеров расположенных за пределами**вашей корпоративной сети, то **лучше купить сертификат** у коммерческого центра. В противном случае, свой центр сертификации – более дешевый, более быстрый и более логичный пусть. Именно эти путем и будем следовать мы, но, как вы могли заметить, Active Directory Certificate Services я не настраивал, поэтому пока выбираю третий вариант.

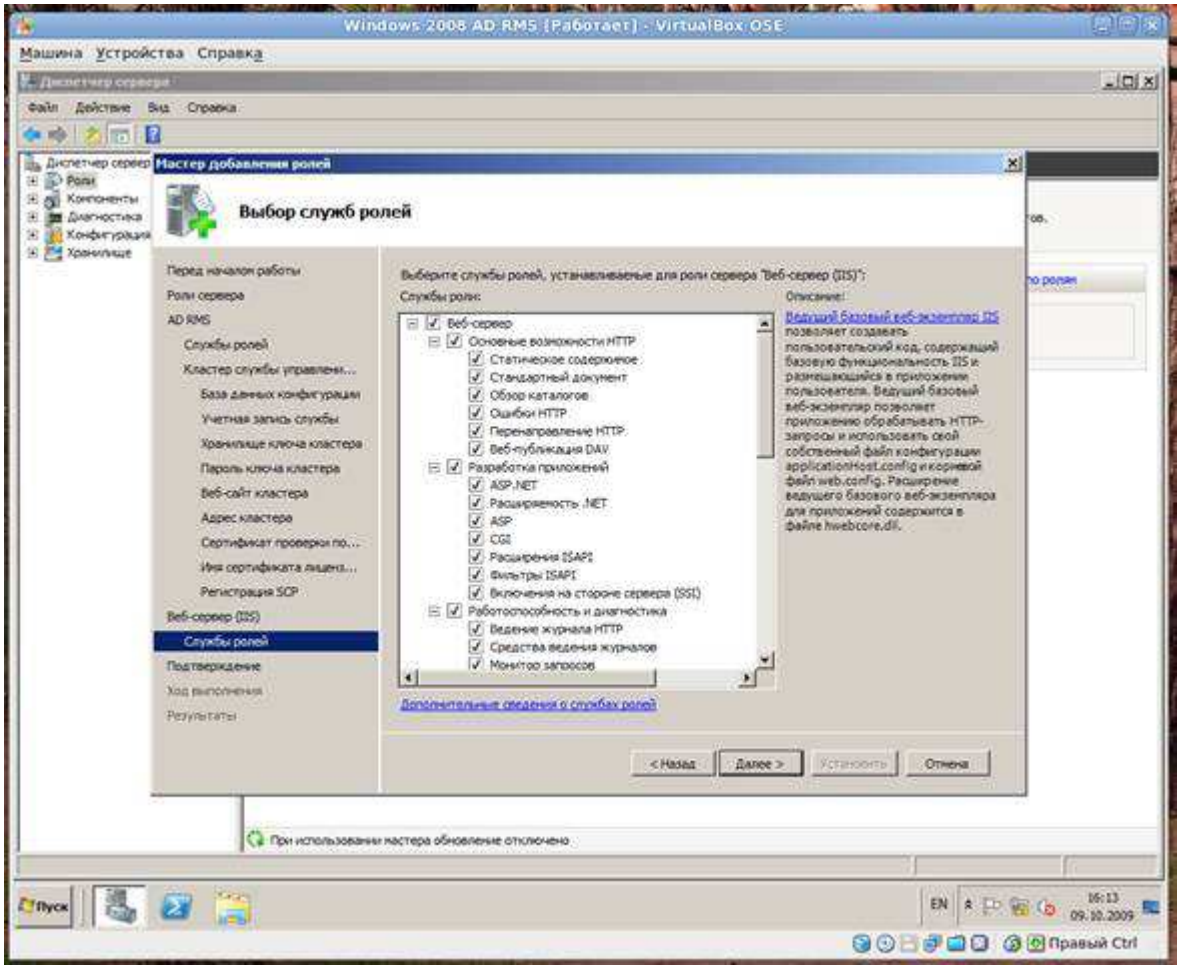
3. **Выбрать сертификат для шифрования SSL позднее.** Установку мы сможем продолжить, но для работыAD RMS сертификатом придется разжиться позднее.



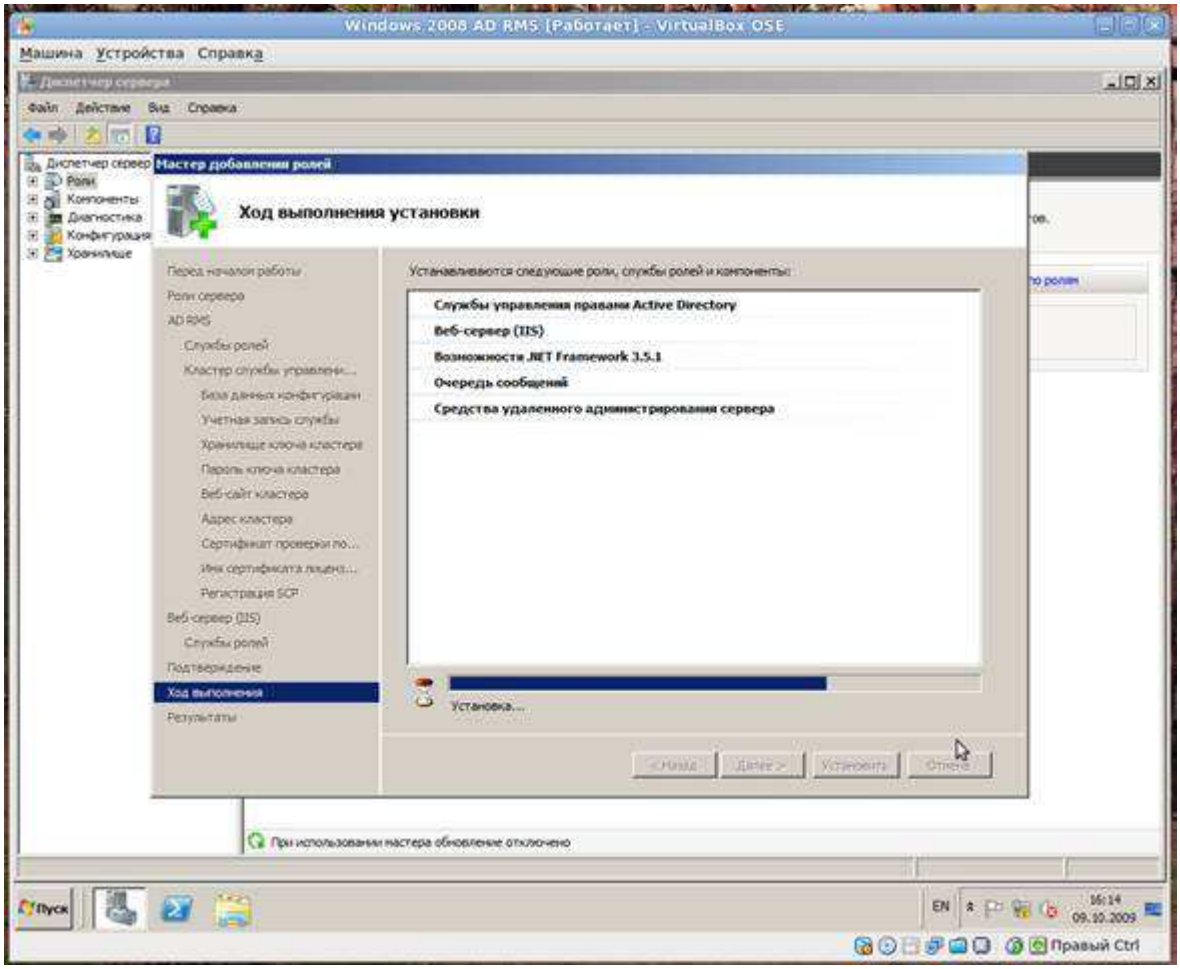
Вводим имя AD RMS кластера, оно должно быть простым и понятным, по умолчанию именем кластера является имя первого сервера.



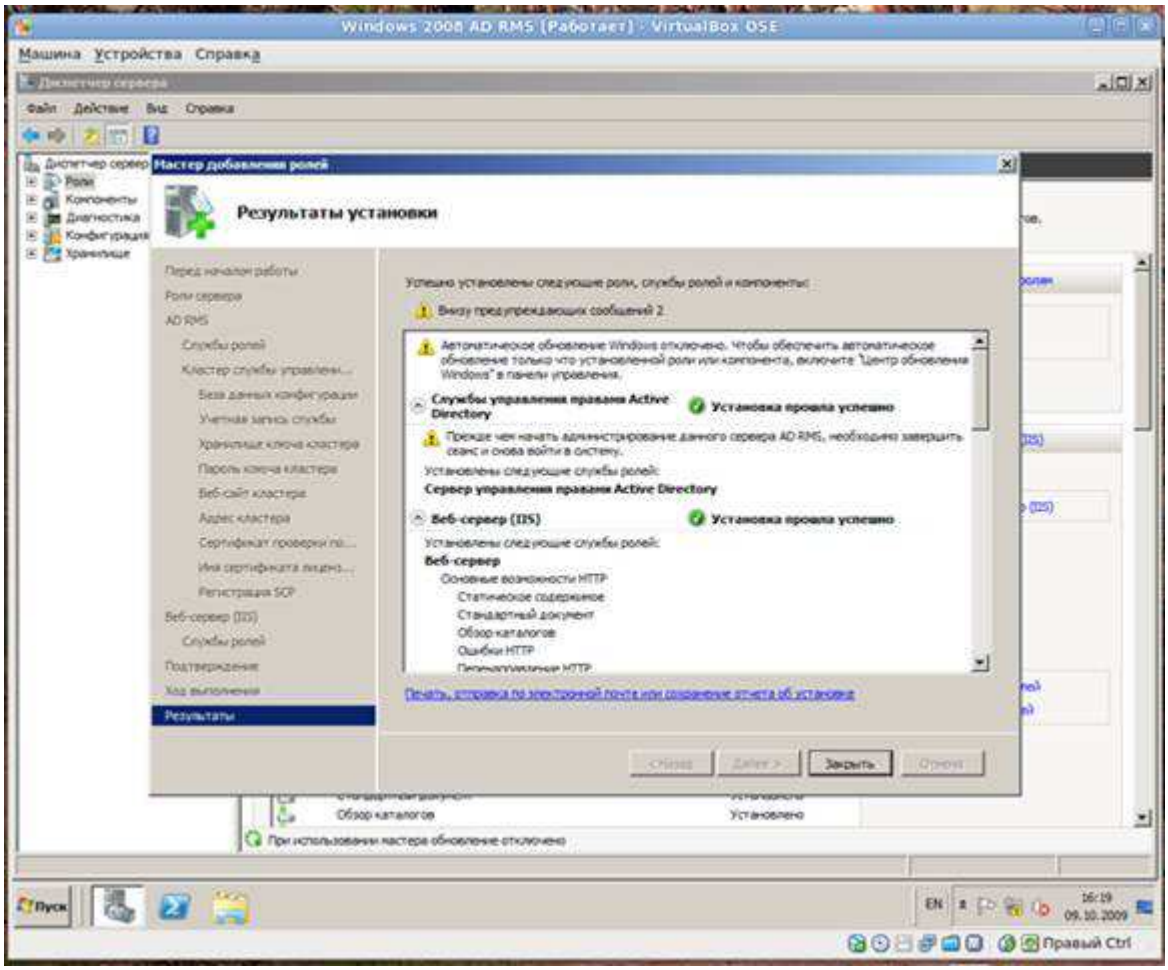
Далее мастер спрашивает, регистрировать ли сейчас **точку подключения службы** AD RMS. **Service connection point** (**SCP** или **точка подключения**) не что иное, как запись URL-а (ссылки) на ваш кластер, которая хранится в базе AD DS и естественно будет доступна членам вашего домена, которые могут захотеть к этому кластеру подключиться. И вот когда они захотят, то возьмут URL кластера прописанный в SCP. Если процедура установки запущена от учетной записи, входящей в группу **Enterprise Administrators** (Администраторы предприятия), то регистрацию можно выполнить сразу.



Настройки AD RMSзакончены, и мастер переходит к веб-серверу IIS. IIS 7 в Windows 2008 стал до неприличия модульным и предлагает указать, какие компоненты необходимо установить. В оригинальной инструкции по установке AD RMS предлагается оставить компоненты, заданные мастером установки и перейти далее. Я же в своей инсталляции выбрал все компоненты, кроме FTP-сервера.

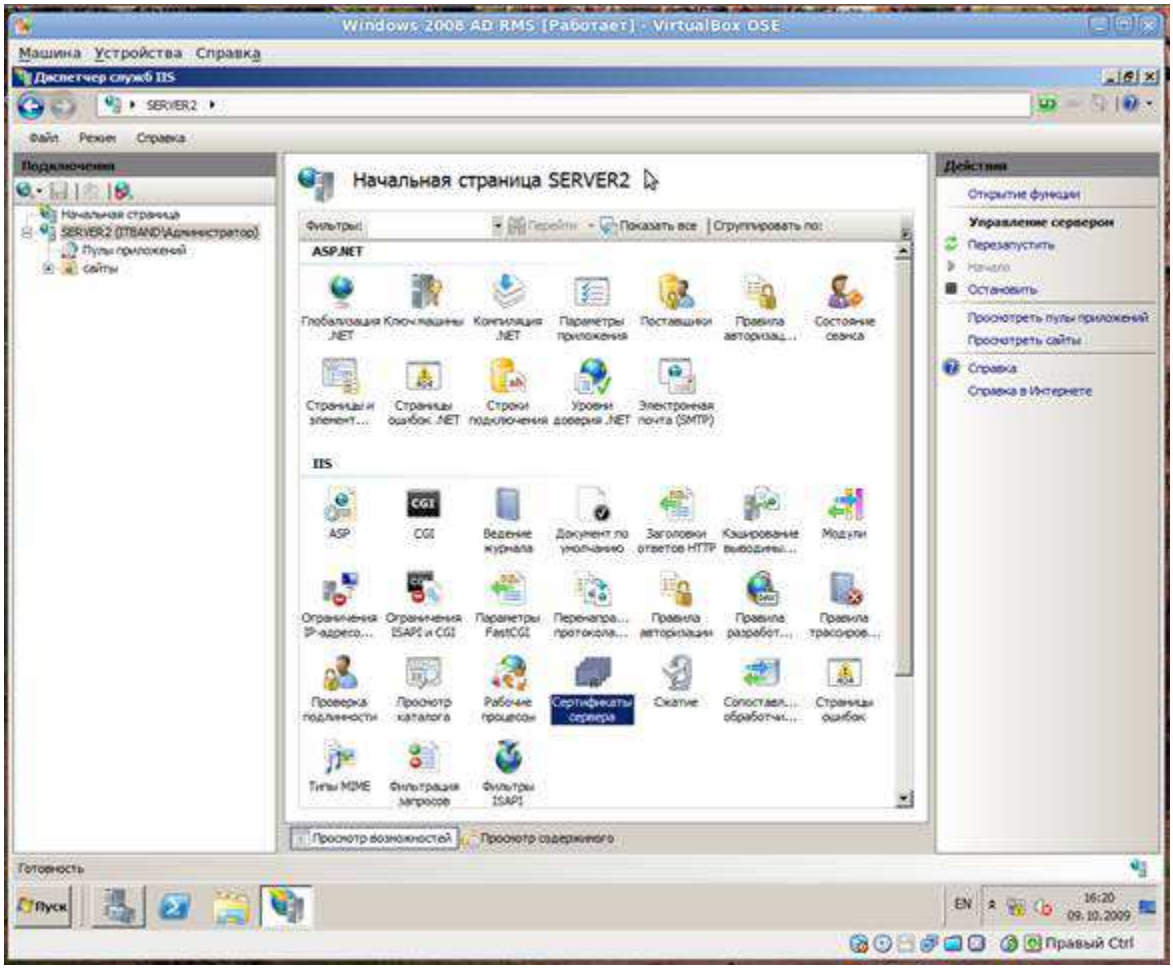


Все параметры введены, и стартует мастер установки, чьего окончания работы необходимо дождаться.

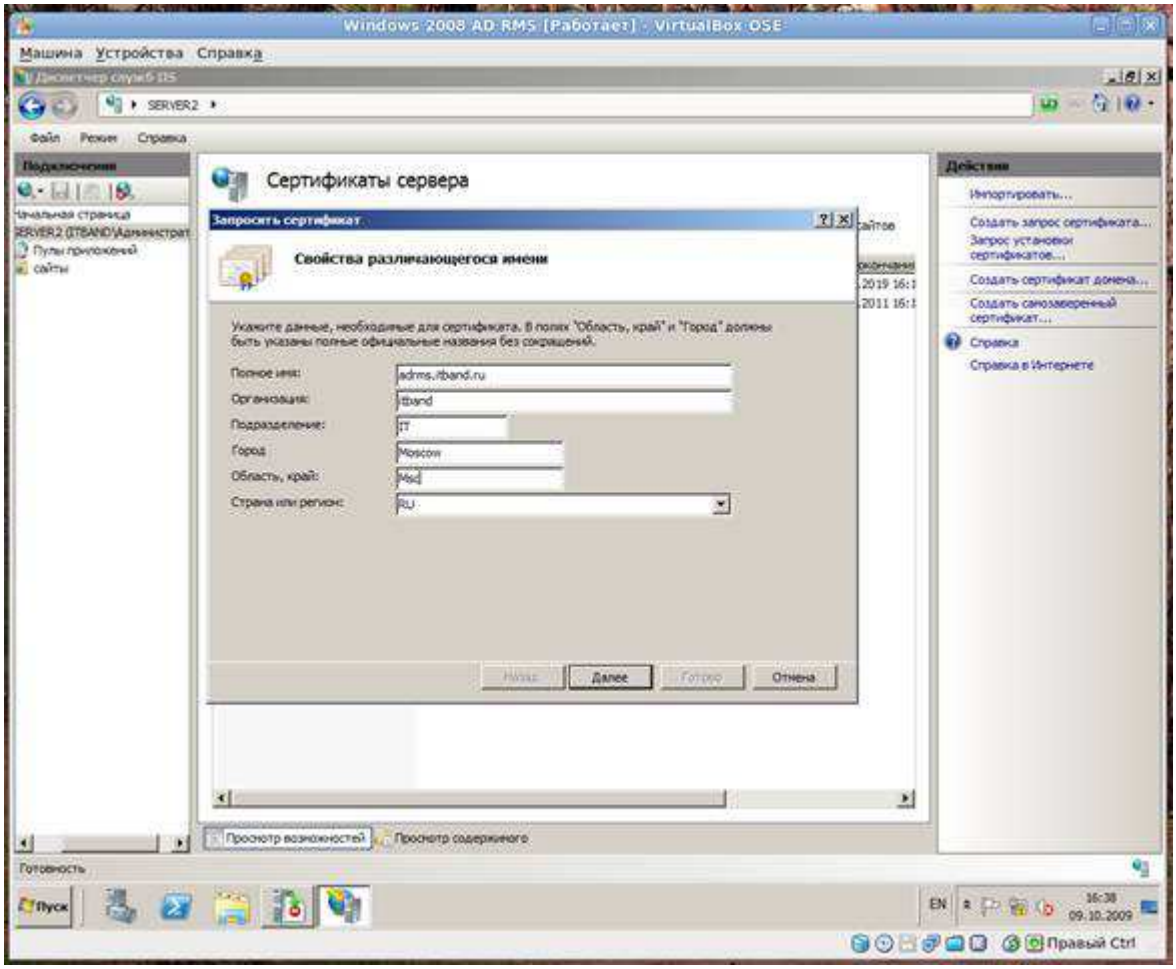


Если вы все делали правильно, и луна находилась в нужной фазе, по окончанию работы мастера установки должно появиться окно, говорящее об успешности добавления ролей и необходимости завершения сеанса с повторным входом перед дальнейшей работой с AD RMS.

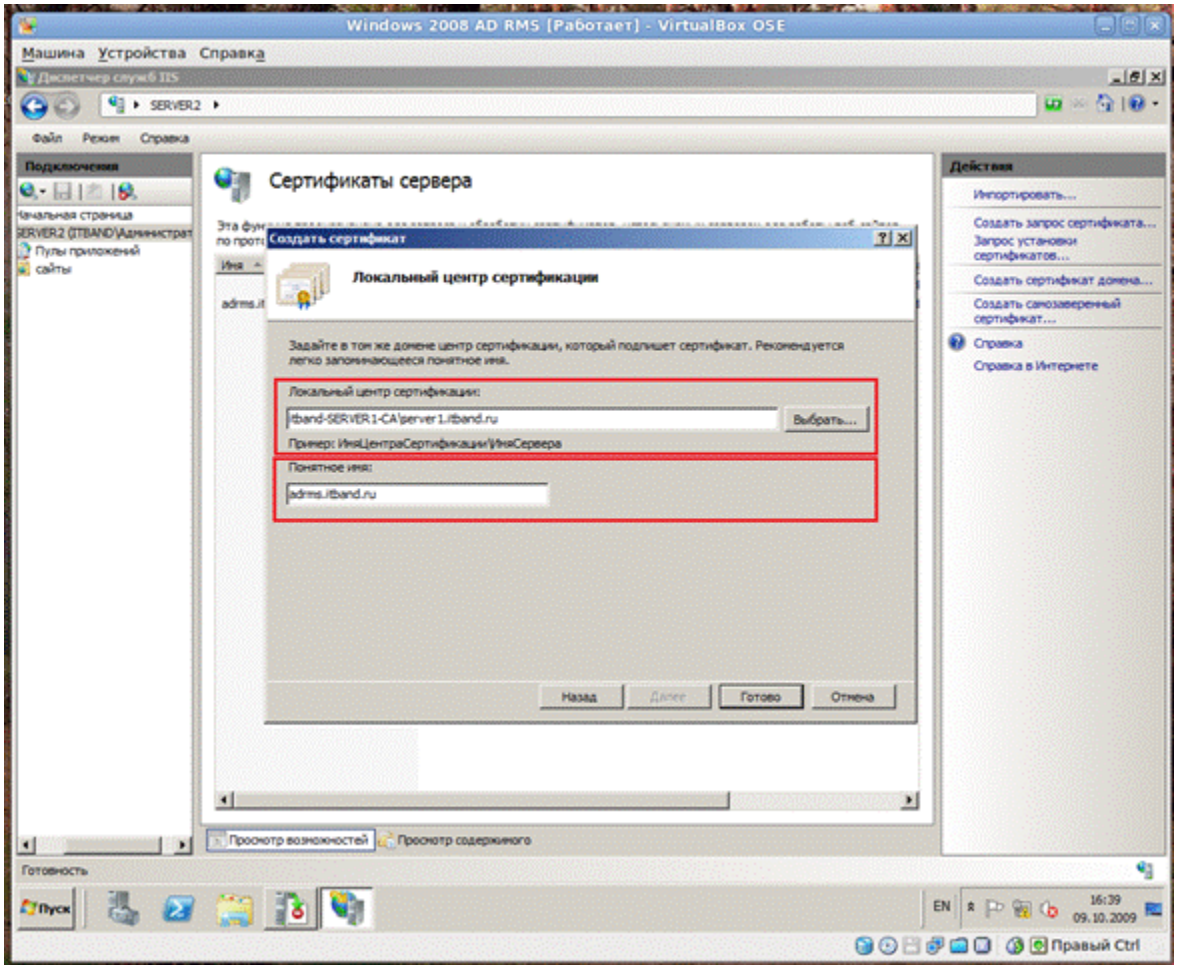
Теперь главной задачей является получение сертификата для веб-сервера IIS, используемого нашей службой AD RMS. Поскольку я не собираюсь покупать сертификат, то на Server1 добавляю роль **Active Directory Certificate Services**. Никакого дополнительного конфигурирования она не потребует, но если у вас возникнут с ней трудности, то скачиваем видео“Установка AD CS”.



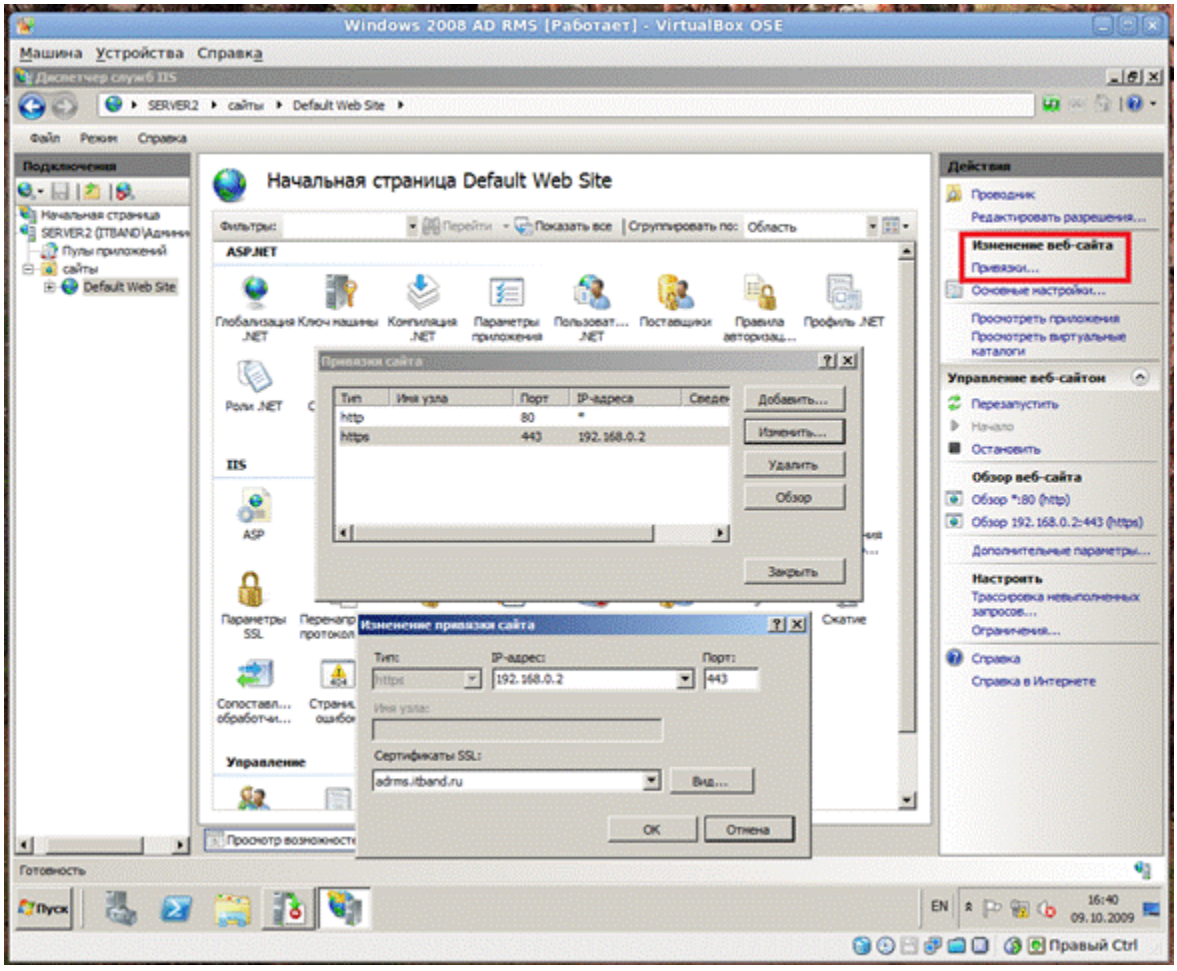
Установив **Службу Сертификации** на Server1, возвращаемся на AD RMS (Server2) и открываем оснастку **Диспетчер служб IIS**. В ней на уровне веб-сервера ищем значок **Сертификаты сервера** и запускаем его.



В действиях выбираем «Создать сертификат домена» и заполняем необходимую для сертификата информацию. Полное имя должно нести FQDNвашего кластера AD RMS. В противном случае, при подключении к кластеру вы получите ошибку, говорящую о том, что сертификат был выдан совершенно для другого узла. Делаем все правильно и следуем далее.



В следующем окне надо задать два блока, первый определяет центр сертификации; если все работает нормально, то задать его можно по кнопке «Выбрать».Второй блок – «Понятное имя»– имя данного сертификата, по которому его сможет легко отличить администратор.



Если предыдущий шаг завершился успешно, на вашем сервере появился выданный сертификат, но пока он не используется. Это положение легко исправить, открыв Default Web Site и выбрав действие «Привязки». В открывшемся окне изменяем подключение по https, указав прослушиваемый IP-адрес и используемый сертификат.Если возникли трудности с оснасткой IIS – качаем видео «Запрос и установка сертификата для IIS».

Вот и все, развертывание службы AD RMS завершено. Что дальше? Дальше будет установка через **Групповые политики** на старые ОС клиента RMS, прописывание адресов

AD RMS: Часть 2 – защита документов
Илья Рудь

В первой части мы развернули серверную часть Active Directory Rights Management Services и теперь пришло время пустить ее в ход. С помощью RMS мы будем защищать стандартные форматы документов, создаваемые пакетом Microsoft Office 2007. В ходе дальнейших экспериментов нам понадобится клиентская ОС. Для этих целей я установил Windows 7 с Enterprise-версией офиса на борту. Напоминаю, что все ОС моложе Windows Vista SP1 требуют установки специального RMS-клиента, скачиваемого с сайтаMicrosoft.

Windows Rights Management Services Client на текущий момент имеет второй пакет обновлений и загружается в зависимости от архитектуры вашей системы.

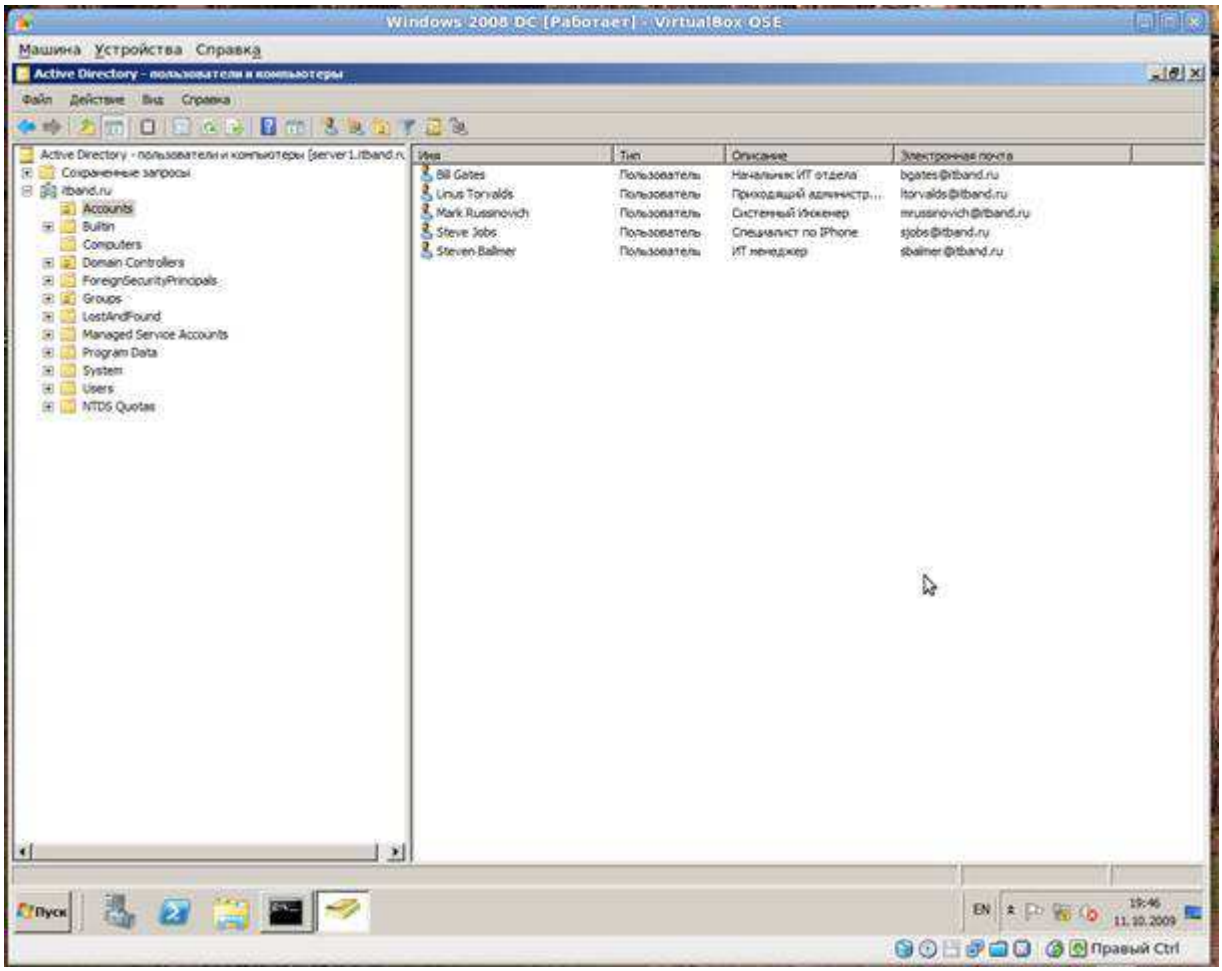
Клиент управления правами Microsoft Windows (SP2) x86

Клиент управления правами Microsoft Windows (SP2) x64

Клиент управления правами Microsoft Windows (SP2) IA64

Поскольку я использую Windows 7, то хлопоты с установкойRMS-клиента меня обошли стороной. Свой клиентский компьютер я включил в домен,предварительно настроив сеть следующим образом: IP- 192.168.0.3; Маска –255.255.255.0; DNS – 192.168.0.1

Для экспериментов мне понадобится несколько учетных записей,каждая из которых обязана иметь заполненный атрибут «электронный ящик».

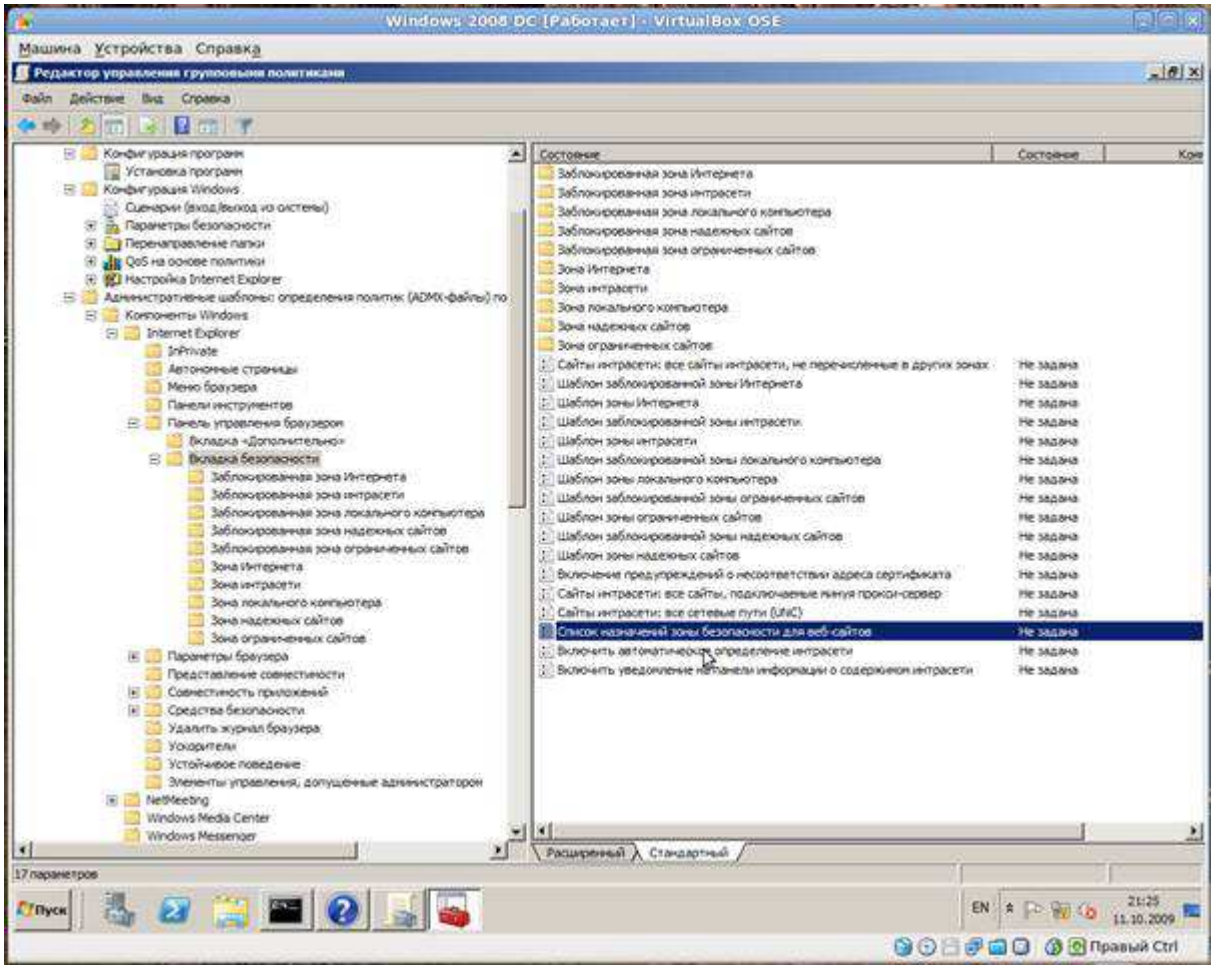


Поэтому я создал новое организационное подразделение **Accounts** и пять учетных записей с прописанными эл. адресами. В моей сети отсутствует Exchange-сервер, посему были прописаны адреса почты, хранящейся у провайдера. Прошу заметить, что все учетные записи имеют полномочия обыкновенных доменных пользователей.

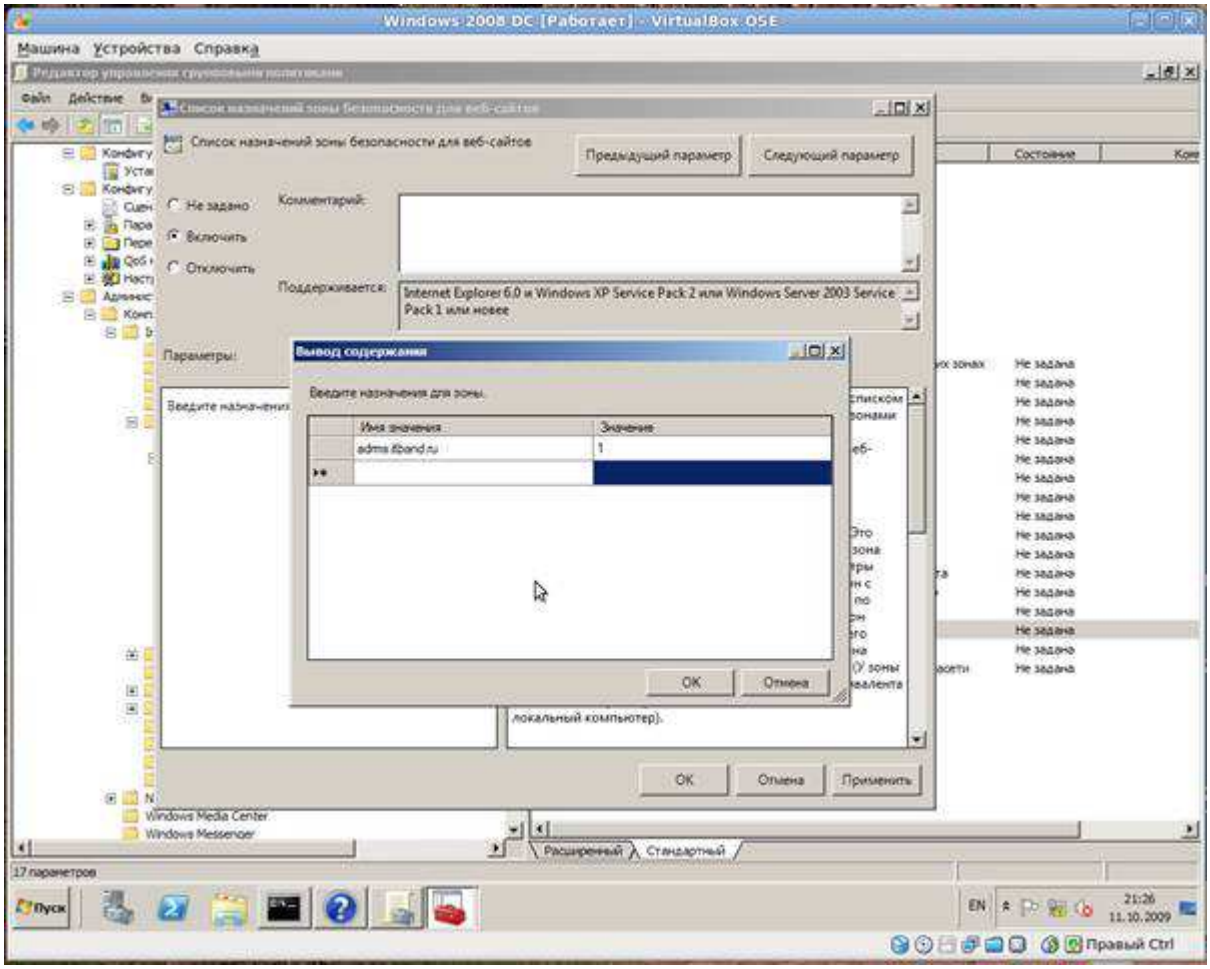
Перед тем как перейти к защите документов, мы должны выполнить еще одно действие – добавить узел adrms.itband.ru (а мы помним, что это имя нашего rms-кластера) в список узлов **Местной Интрасети** клиентских браузеров **IE 8**. Зачем это делается? Когда клиент пытается защитить документ,он обращается по протоколу **https** к кластеру AD RMS, и если узел кластера

не вписан в местную интрасеть, у пользователя повторно запрашивается имя и пароль. Нам это естественно не нужно.

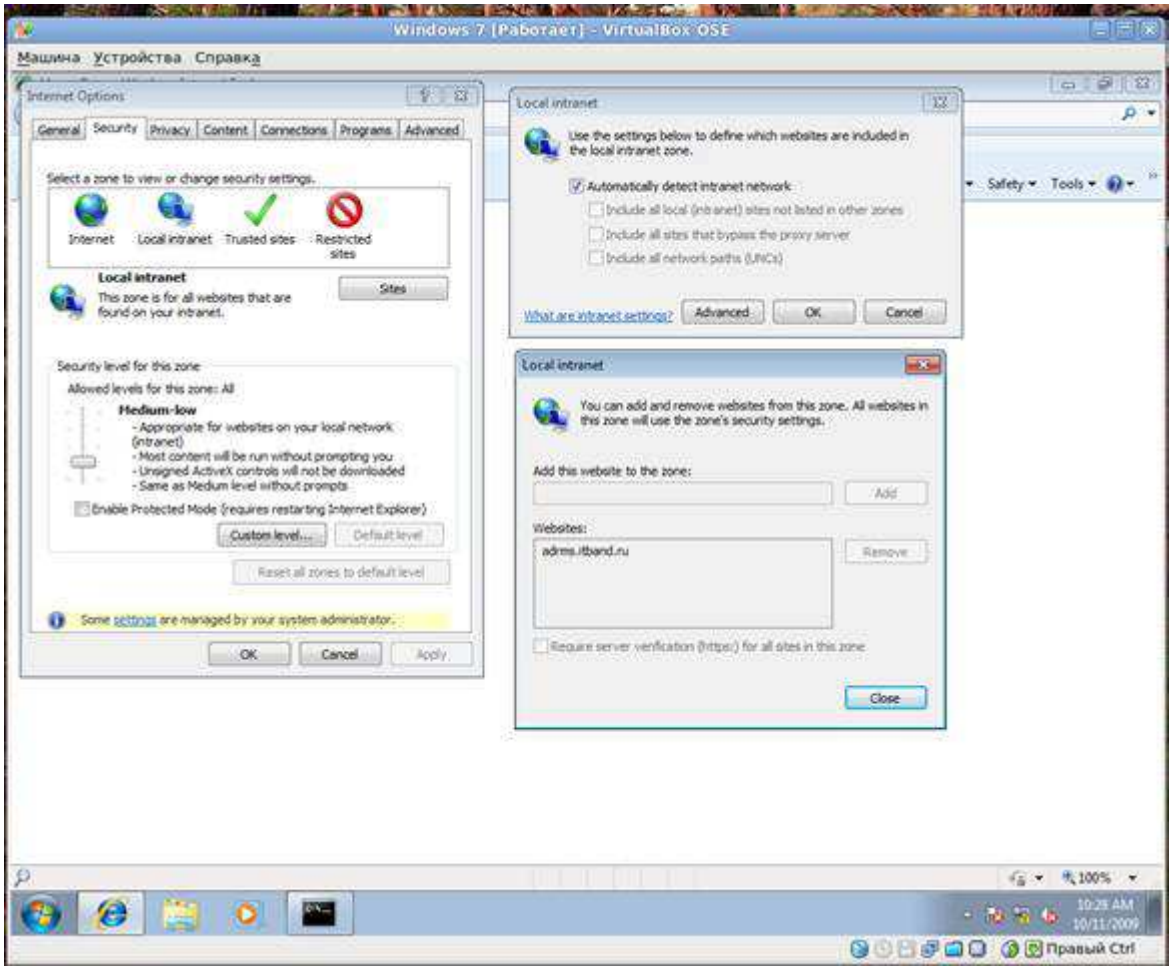
Чтобы максимально автоматизировать процесс добавления,создаем групповую политику «**IE Security Zone**» и прицепляем ее к организационному подразделению **Accounts**.



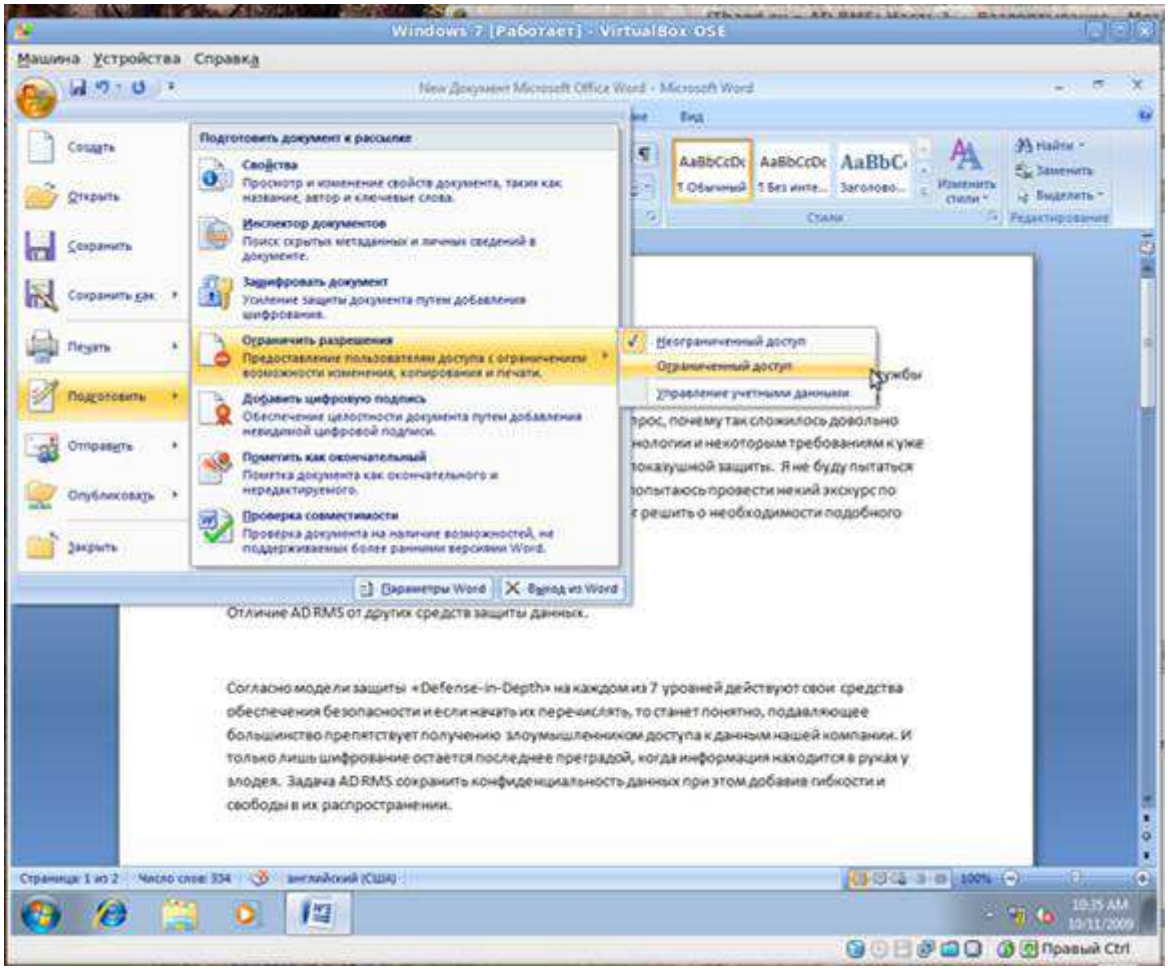
В этой политике разворачиваем: Конфигурацию Пользователя–> Административные Шаблоны –> Компоненты Windows –> Internet Explorer–> Панель Управления браузером –> Вкладка Безопасности –> **Список назначений зоны безопасности для веб-сайтов**.



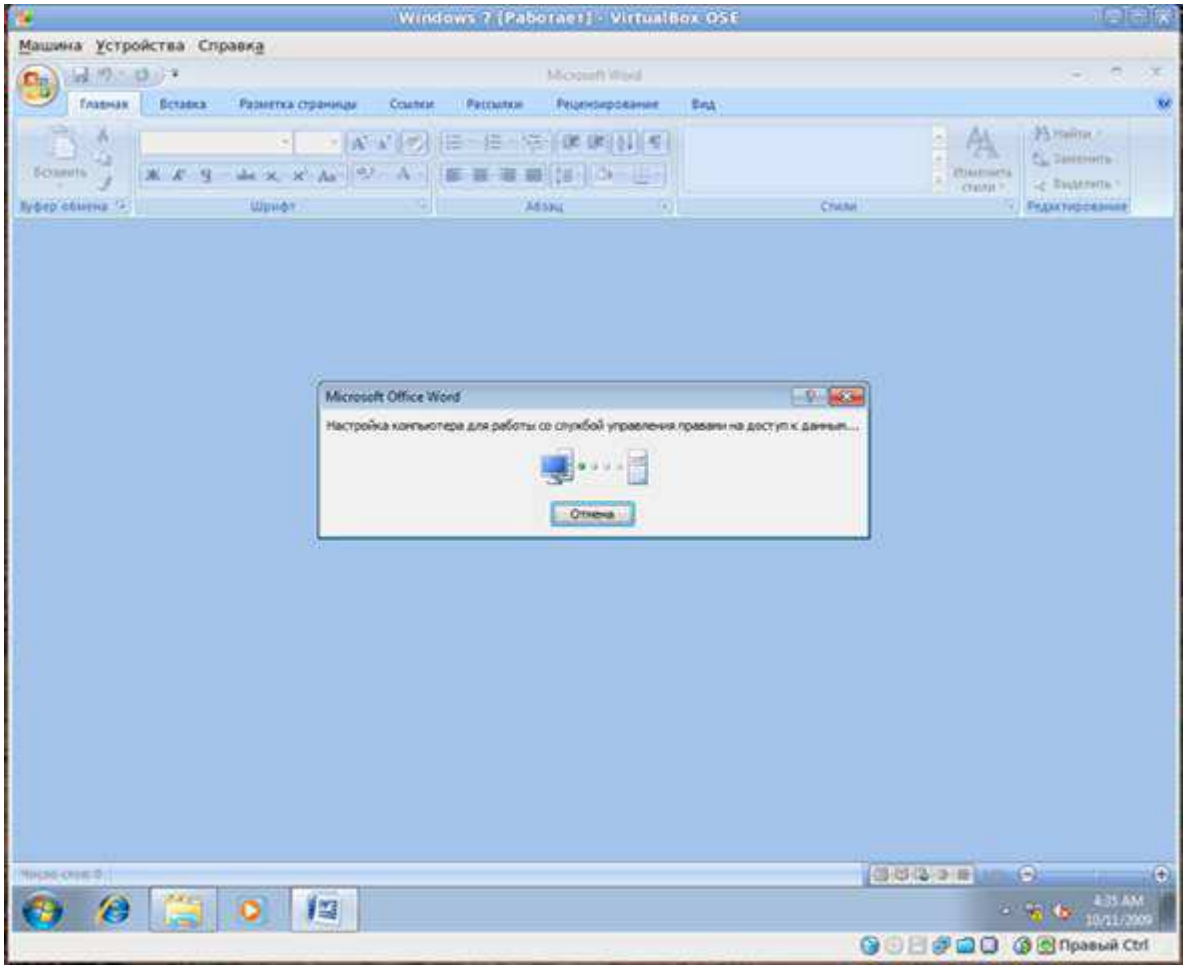
Включим данный параметр и прописываем для узла **adrms.itband.ru** значение равное единице. (1) – это код зоны **Местной Интрасети**, о других кодах можно прочитать в справке, идущей вместе с параметром политики.



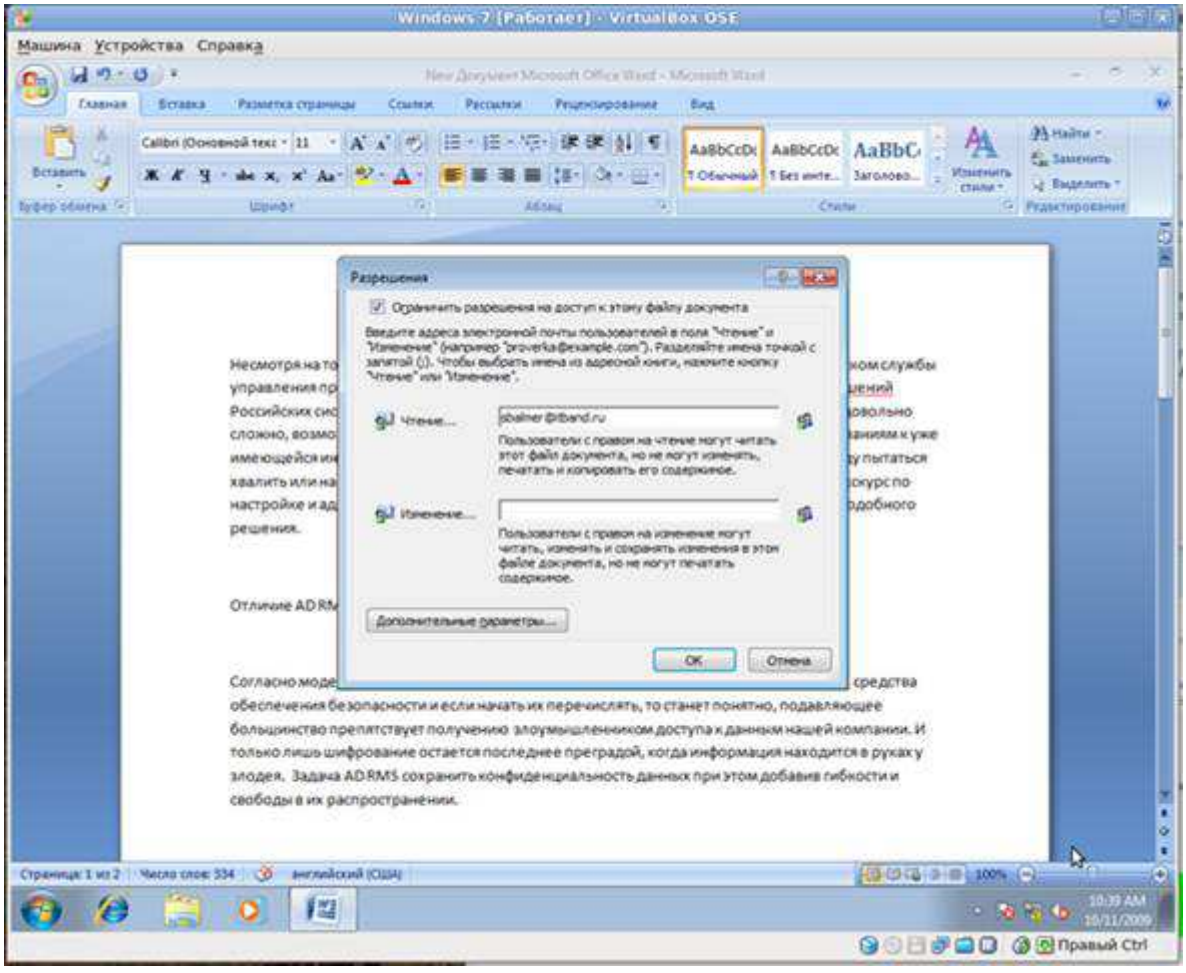
Создав политику, применяем ее на клиенте, путем запуска команды **gpupdate /force** и проверяем результат. В настройках IE8 на клиенте имя нашего кластера должно быть в **Местной Интрасети**.



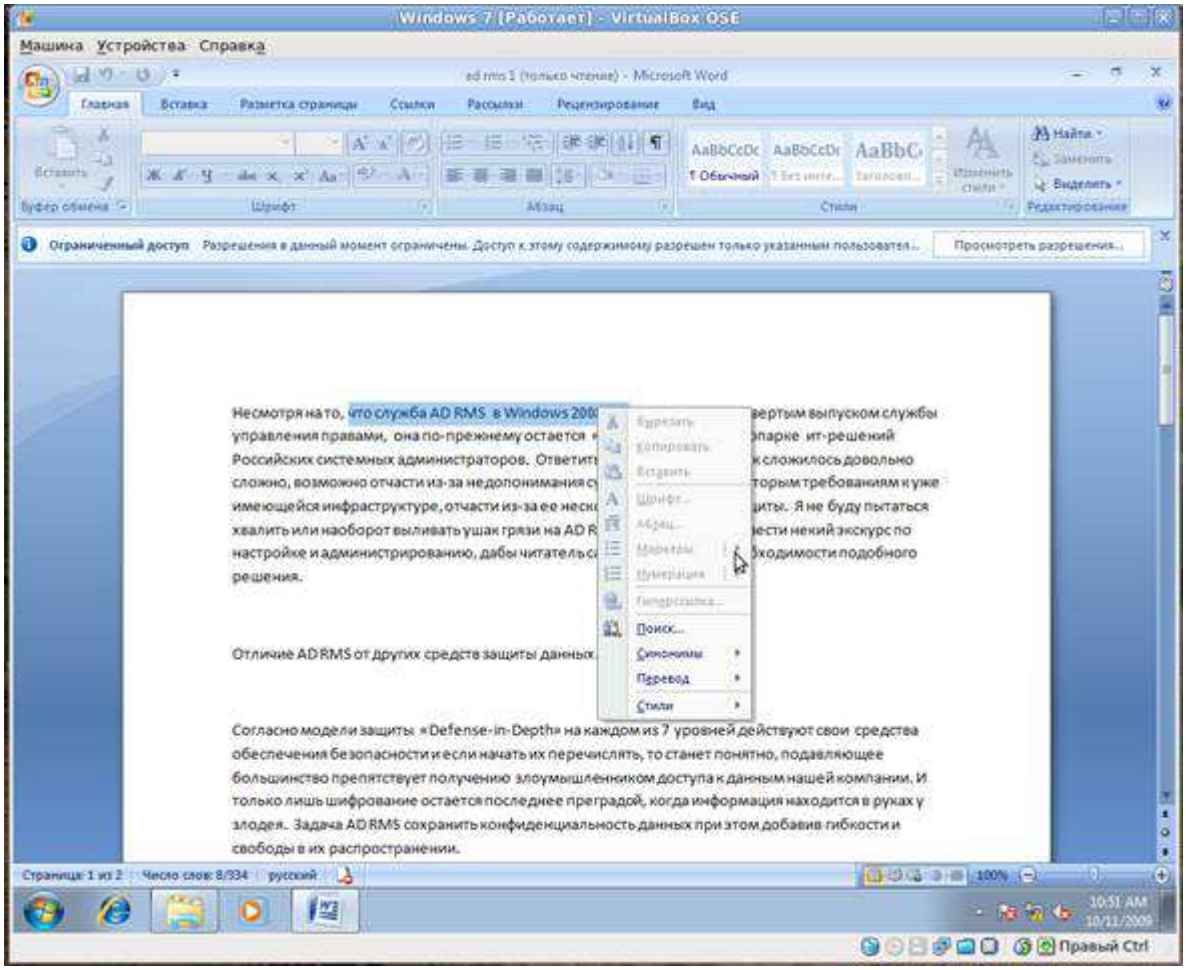
Теперь все готово для проверки RMS. Выполняем вход наWindows 7 от имени учетной записи **Bgates**и создаем тестовый документ **Word 2007**.Как только он будет готов, выбираем в меню опцию «Подготовить»–> «Ограниченный доступ».Если данной опции вы не видите, значит на вашей рабочей станции стоит младший выпуск офиса и вам стоит еще раз вернуться к первой части статьи и посмотреть,с помощью каких выпусков можно защищать документы.



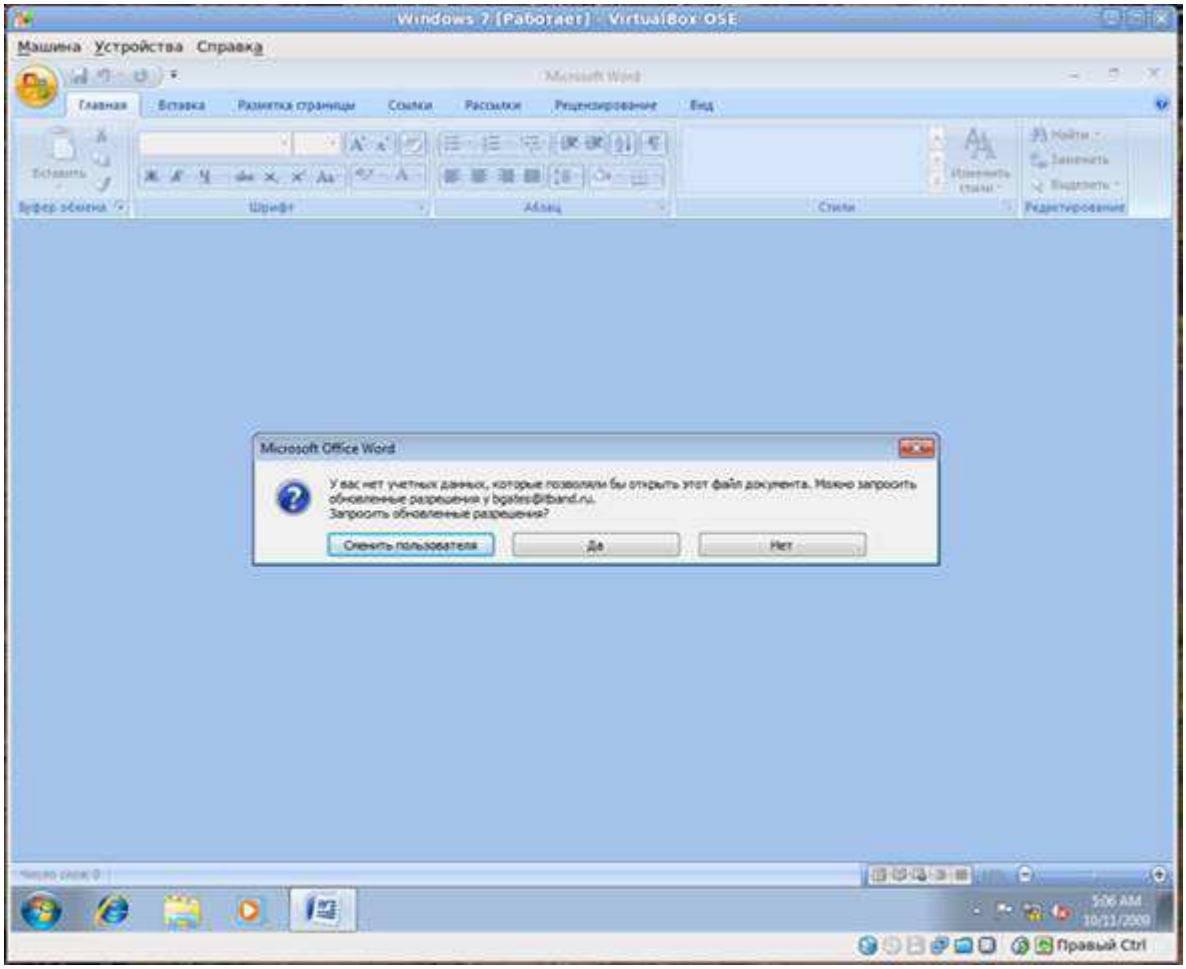
При первой попытке защитить документ ваш компьютер запустит процедуру настройки, и, если у вас все предварительные шаги выполнены правильно, то результатом будет вывод окна ограничения прав.



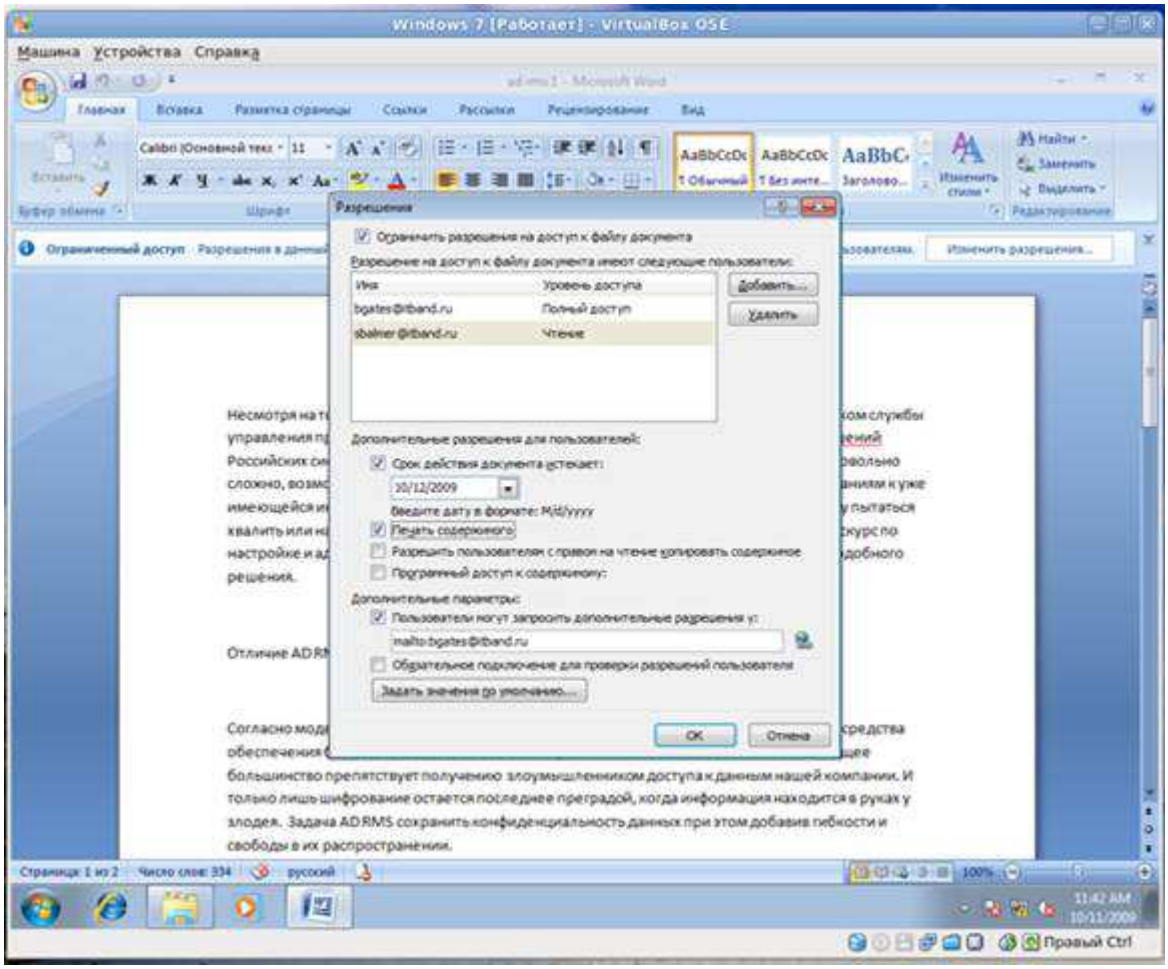
Начнем с простого, разрешим только «**Чтение**» и только одной учетной записи **Sbalmer**, прописав в поле чтение его электронный адрес. Сохраняем документ в доступное учетной записи Sbalmer место и выполняем под ней вход.



Открыв тот же самый документ под пользователем **Sbalmer,** видим появившееся предупреждение об ограничение доступа к данному документу. Пытаемся изменить,сохранить, скопировать и видим, что сделать этого не удается. Тем кто думает,что клавиша **Print Screen** спасет отцов **«**русской демократии»сразу отвечу: не спасет! **Print Screen**не работает. И вам остается либо смириться с данными правами, либо запросить дополнительные разрешения у автора документа, отослав ему письмо по электронной почте.

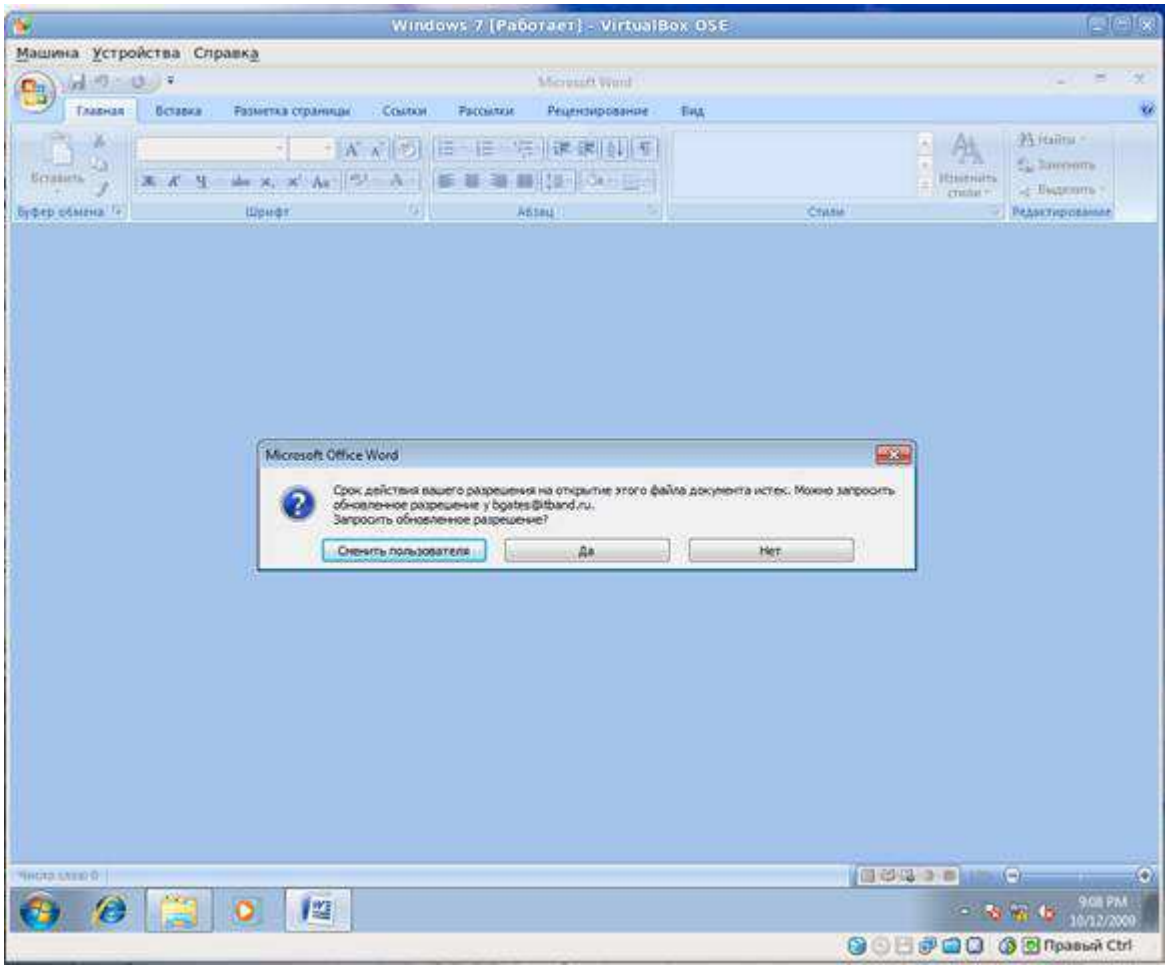


Может возникнуть вопрос: **что же увидит человек, у которого вообще нет прав на данный документ**?А увидит он сообщение о невозможности открыть файл, по причине отсутствия полномочий. И предложение эти права запросить. Учтите, что в **NTFS** разрешения на данный документ могут быть хоть **Full**, но это никак не поможет получить доступ к его содержимому.



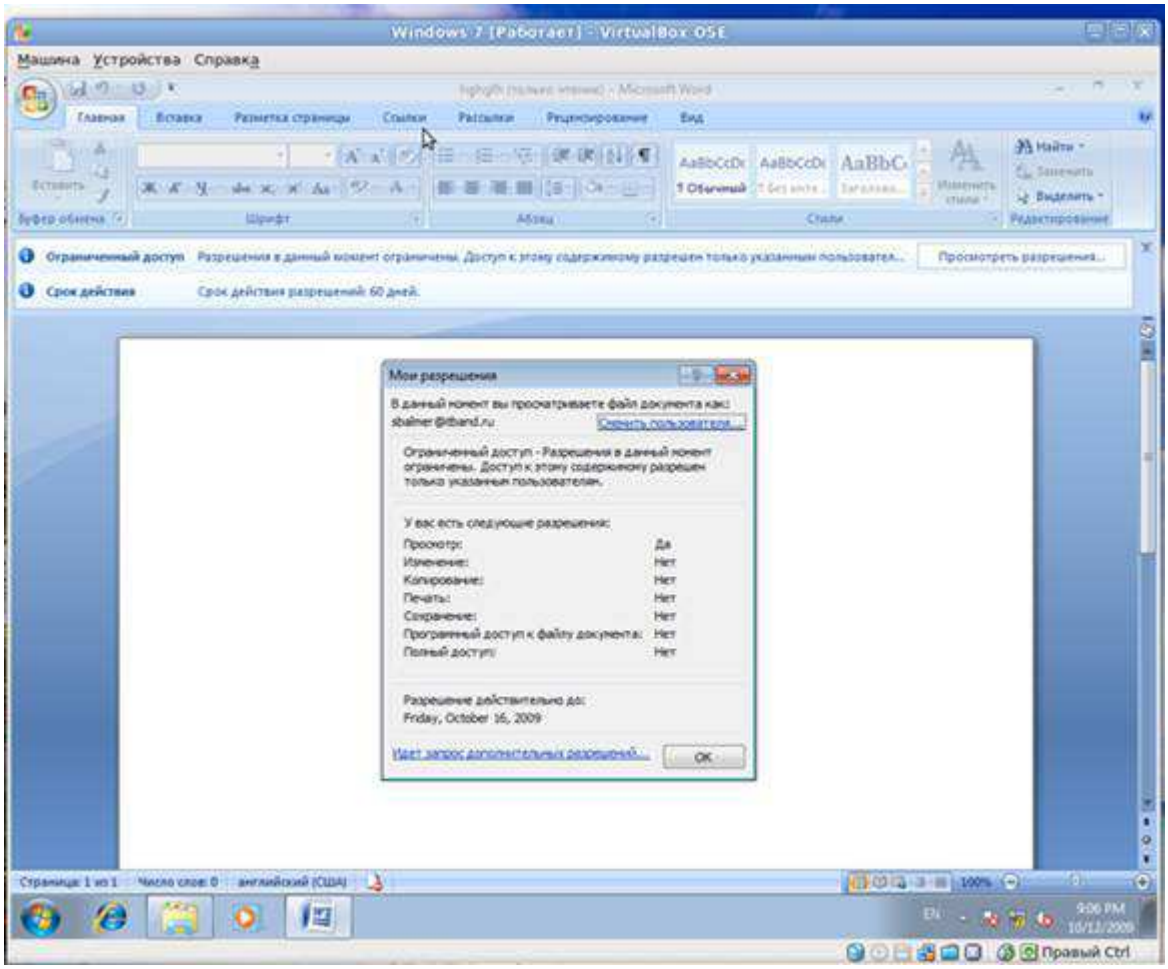
Снова заходим под учетной записью **Bgates** и открываем «Ограничение разрешений»,только теперь с дополнительными параметрами. Из появившихся любопытных прав:разрешить **Печать содержимого** и **ограничить срок жизни документа**. Если по печати все понятно, то срок действия документа рассмотрим подробней.

Срок действия документа указывает, как долго будут действовать установленные ограничения.По окончанию срока жизни доступ к документу сможет получить только пользователь, имеющий «**Полный Доступ»**.



Все остальные получают сообщение об истечении срока разрешений. Звучит красиво, но я столкнулся с некоторыми трудностями.

Трудность первая: **запоздалая реакция**. Мною был создан документ и установлены разрешения со сроком до 12октября. После чего я открыл документ 12 октября в 00:08 и с удивлением обнаружил, что он по-прежнему доступен. Поскольку это был час ночи, продолжать изыскания не хотелось. Утром же вернувшись к этому документ снова, я получил сообщение об истекшем сроке разрешений, т.е. права сработали.



Трудность вторая: **странное поле**. Открывая защищенный документ можно увидеть свои права, в том числе и до какого числа они действительны. Мне на данный момент не ясно, что значит «Срок действия разрешений 60 дней», указанный выше. Логически я понимаю,что там должно быть количество дней до часа X. (На картинке 16 октября). Откуда взялись 60 дней?

Вывод. Со сроком действия разрешений нужно разбираться и разбираться, если кто прояснит ситуацию, я буду очень благодарен.

И еще одна капля дегтя. Все свои эксперименты я провожу в виртуальной среде, каждая виртуальная машина имеет по 1.5 Gb оперативной памяти и находится на личном жестком диске. Когда я открываю защищенный документ, либо защищаю новый, время на открытие или защиту документа иногда превышает 45–50 секунд. И это при условии,что между компьютерами нет медленных каналов. Я допускаю, что это особенности виртуализации, но очень похоже на тормоза «by design». Пока вывода сделать не могу,но если это норма, сотрудники будут «не рады» однозначно.

Важно понять следующее:

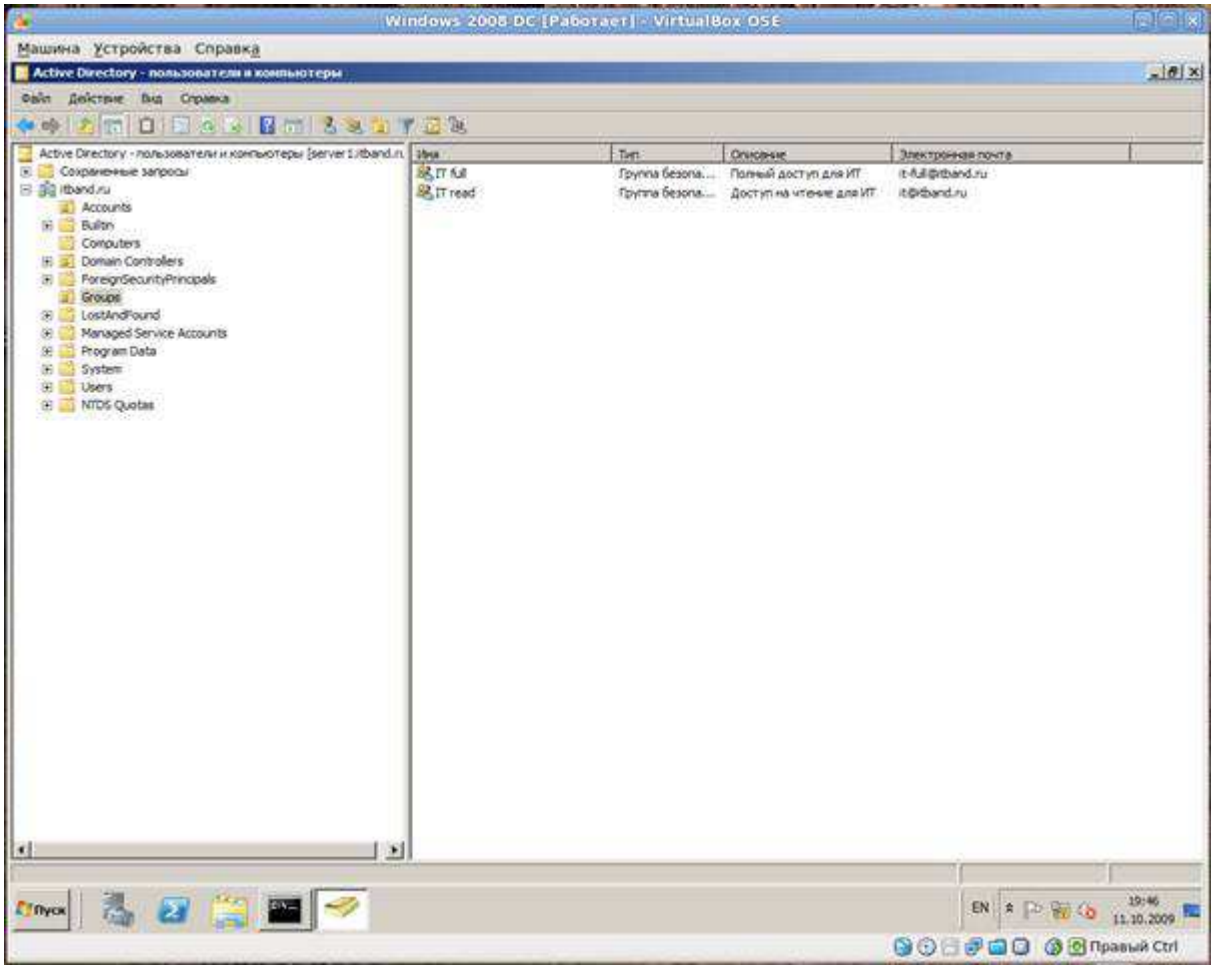
1. Разрешения можно давать **как пользователям**, так и любым **группам Безопасности**. Главное, чтобы эти группы имели заполненный атрибут «эл.ящик». Соответственно, разрешения будут действовать на членов этой группы.

2. Большинство пользователей не будет разбираться с расширенными разрешениями, поэтому наша цель – свести их клики к минимуму.

Давайте сформируем примитивную задачу: **Bgates** является начальником ИТ-отдела и ежедневно распространяет среди своих сотрудников документы. Он хочет чтобы ИТ-сотрудники имели одно право – на чтение этих документов. Все остальные не могли бы даже открыть его приказы.

В тоже время в отделе есть ИТ-менеджер **Sbalmer**, который имеет высокую степень доверия и должен на некоторые документы иметь полные права.

Для решения этой задачи создаем две группы безопасности: **IT full** и **IT Read**.



В **IT Read** у нас входят все пять членов отдела: bgates, sbalmer, sjobs, mrussinovich, ltorvalds.

В **IT full** только:bgates, sbalmer.

Естественно, что каждая из групп имеет электронный адрес.Как быть дальше? Все очень просто – создать шаблоны прав, которые впоследствии сотрудник (в нашей ситуации – начальник отдела bgates) будет выбирать при защите документов. Но об этом мы поговорим в третьей части серии статей поActive Directory Rights Management Services.

AD RMS: Часть 3 – Шаблоны
Илья Рудь

Продолжаем разговор об AD RMS. Напомню, что в конце второй части я пришел к выводу о сложности установки разрешений на документы для обыкновенных пользователей и необходимости автоматизации этой задачи. В AD RMS существует такое понятие как «шаблон RMS», иначе говоря, заготовка или шаблон прав, который может быть применен к любому документу. Что сильно облегчает жизнь, упрощая защиту документа до выбора необходимого шаблона. Самым сложным этапом внедрения шаблонов является планирование. И для начала я предлагаю ознакомиться с подходом к созданию шаблонов самого автора AD RMS, а именно корпорацииMicrosoft.

Не буду изобретать велосипед и приведу перевод Артема Синицына информации от Microsoft в качестве примера реализации шаблонов.

Начало цитаты:

Для удобства работы пользователей и упрощения соответствия корпоративным политикам защиты электронных документов специалисты ИТ-отдела софтверного гиганта создали пять шаблонов политик AD RMS. Рассмотрим более подробно каждый шаблон из этой пятерки.

Microsoft Confidential – в качестве участника безопасности в данном шаблоне выступает группа рассылки Microsoft All Staff, включающая в себя всех внутренних сотрудников компании Microsoft (full-time employees, FTE), всех контрактников и сотрудников вендоров. То есть за пределами компании Microsoft защищенная этим шаблоном информация будет *недоступна*,тогда как сотрудники компании будут иметь возможность *полноценно*работать с данными документами.

Данный шаблон предоставляет группе, включающей всех сотрудников компании следующие права доступа:

- View (Просмотр)
- Save (Сохранить)
- Edit (Редактирование)
- Reply (Ответ)
- Reply All (Ответ всем)
- Forward (Перенаправление).

Microsoft Confidential Read Only – в качестве участника безопасности в данном шаблоне выступает группа рассылкиMicrosoft All Staff, включающая в себя всех внутренних сотрудников компанииMicrosoft (FTE), всех контрактников и сотрудников вендоров. То есть за пределами компании Microsoft защищенная этим шаблоном информация будет *недоступна*,тогда как сотрудники компании будут иметь возможность *просматривать*данные документы (доступ только на чтение).

Данный шаблон предоставляет группе, включающей всех сотрудников компании следующие права доступа:

- View (Просмотр).

Microsoft FTE Confidential – в качестве участника безопасности в данном шаблоне выступает группа рассылки Microsoft All FTE, включающая в себя *только*внутренних сотрудников компании Microsoft (full-time employees, FTE). То есть за пределами компании Microsoft, включая всех контрактников и сотрудников вендоров, защищенная этим шаблоном информация будет *недоступна*, тогда как *внутренние* сотрудники компании будут иметь возможность *полноценно*работать с данными документами.

Данный шаблон предоставляет группе, включающей всех сотрудников компании следующие права доступа:

- View (Просмотр)
- Save (Сохранить)

- Edit (Редактирование)
- Reply (Ответ)
- Reply All (Ответ всем)
- Forward (Перенаправление).

Microsoft FTE Confidential Read Only – в качестве участника безопасности в данном шаблоне выступает группа рассылкиMicrosoft All FTE, включающая в себя *только* внутренних сотрудников компании Microsoft (FTE). То есть за пределами компании Microsoft, включая всех контрактников и сотрудников вендоров, защищенная этим шаблоном информация будет*недоступна*, тогда как сотрудники компании будут иметь возможность *просматривать*данные документы (доступ только на чтение).

Данный шаблон предоставляет группе, включающей всех сотрудников компании следующие права доступа:

- View

Do Not Reply All – единственное назначение данного шаблона политикAD RMS – запретить пользователям использовать кнопку «Reply All (Ответить всем)». Полагаю, многим из нас знакомы случаи, когда две секретарши возмущенно и довольно-таки нескромно обсуждают в почтовой переписке политику нового начальства. А эту переписку читает всё подразделение или, что хуже, вся компания, только лишь потому, что девушки нечаянно, или намеренно,нажали «Ответить всем», вместо «Ответить». В общем, данный шаблон является просто незаменимым средством для предотвращения массовых почтовых рассылок.

Конец цитаты.

Теперь вернемся к нашим реалиям, если не забыли в конце второй части перед нами стояла задача обеспечить начальнику ИТ-отдела ***Bgates*** возможность защищать свои документы. При этом сотрудники его отдела должны иметь только одно право – право на их чтение. А все остальные сотрудники компании не могли даже открыть их. Плюс к этому ИТ-менеджер ***Sbalmer***, который имеет высокую степень доверия и должен на некоторые документы иметь полные права.

Для этого мы создавали две группы безопасности:

IT F ull – члены группы: ***bgates, sbalmer***.

IT Read – члены группы**: bgates, sbalmer, sjobs, msussinovich, ltorvalds**

Порядок создания шаблона AD RMS будет следующим:

1. Создать папку с общим доступом, которая будет хранить шаблоны

2. Объяснить Office 2007, что шаблоны он должен брать из папки, созданной в п.1

3. Включить сохранение создаваемых шаблонов в папку из п.1

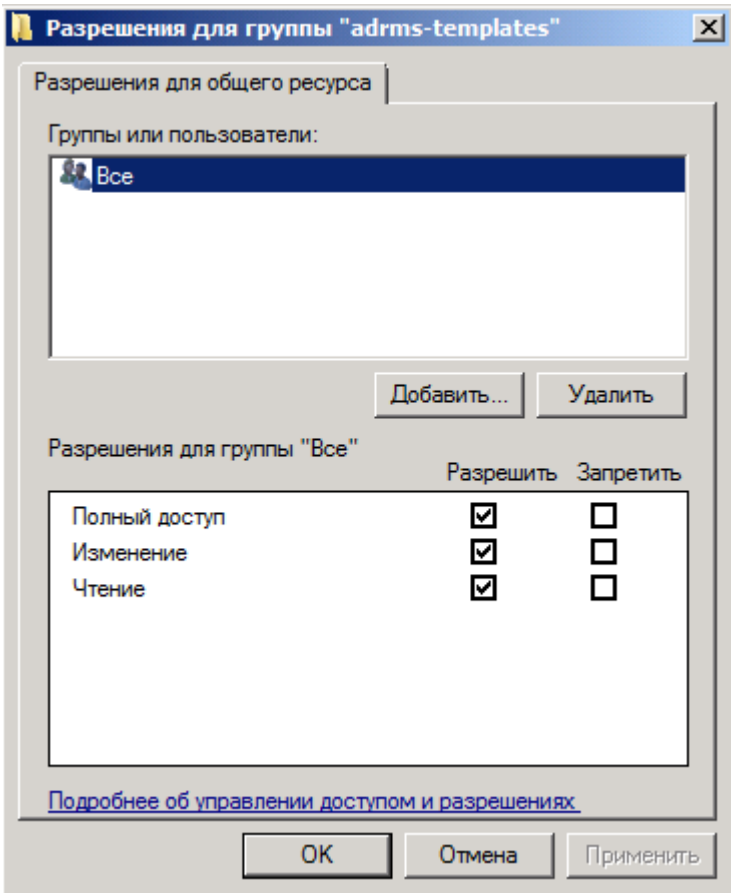
4. Создать два шаблона.

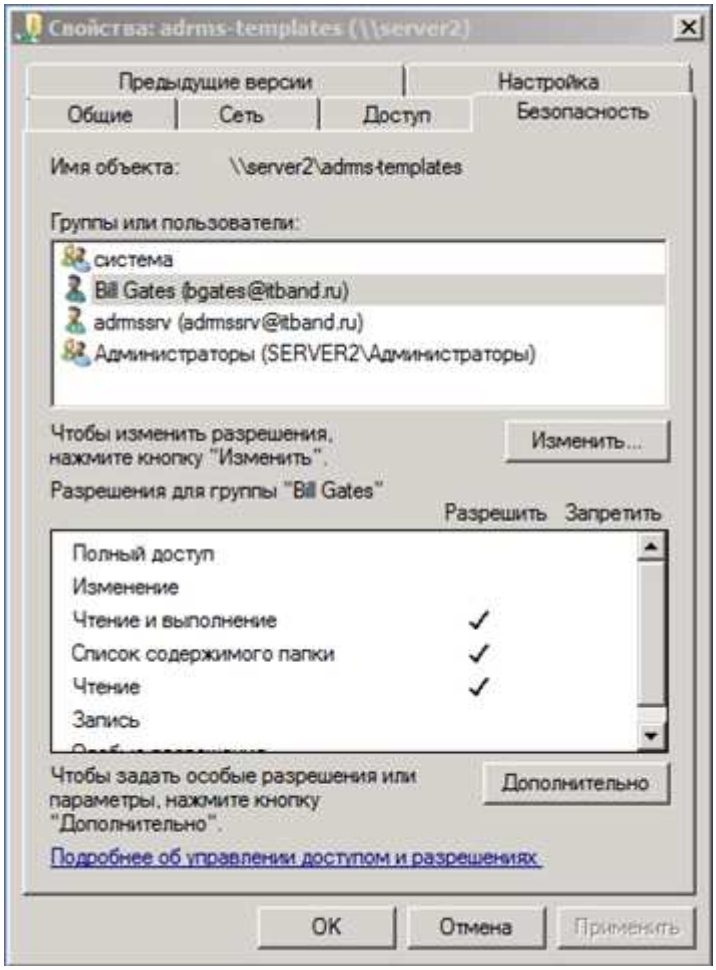
Приступим к настройке шаблонов, для этого зайдем на наш сервер AD RMS и первым делом создадим папку общего доступа(я назову ее ***adrms-templates***). Распространять шаблоны можно несколькими способами. Есть вариант доставлять шаблоны на клиента через групповые политики, я же пойду другим путем и создам центральное хранилище шаблонов.

Открывая доступ к папке, я предлагаю дать ***следующие права****:*

– Права общего доступа. Группе Все – Полный доступ.

– ***Права NTFS.*** Учетной записи, от которой работает служба AD RMS (у меня ***adrmssrv***) даем права «**Изменение**». А пользователю «***bgates***», т.е тому кто с помощью шаблонов будет защищать документы – «**Чтение**».



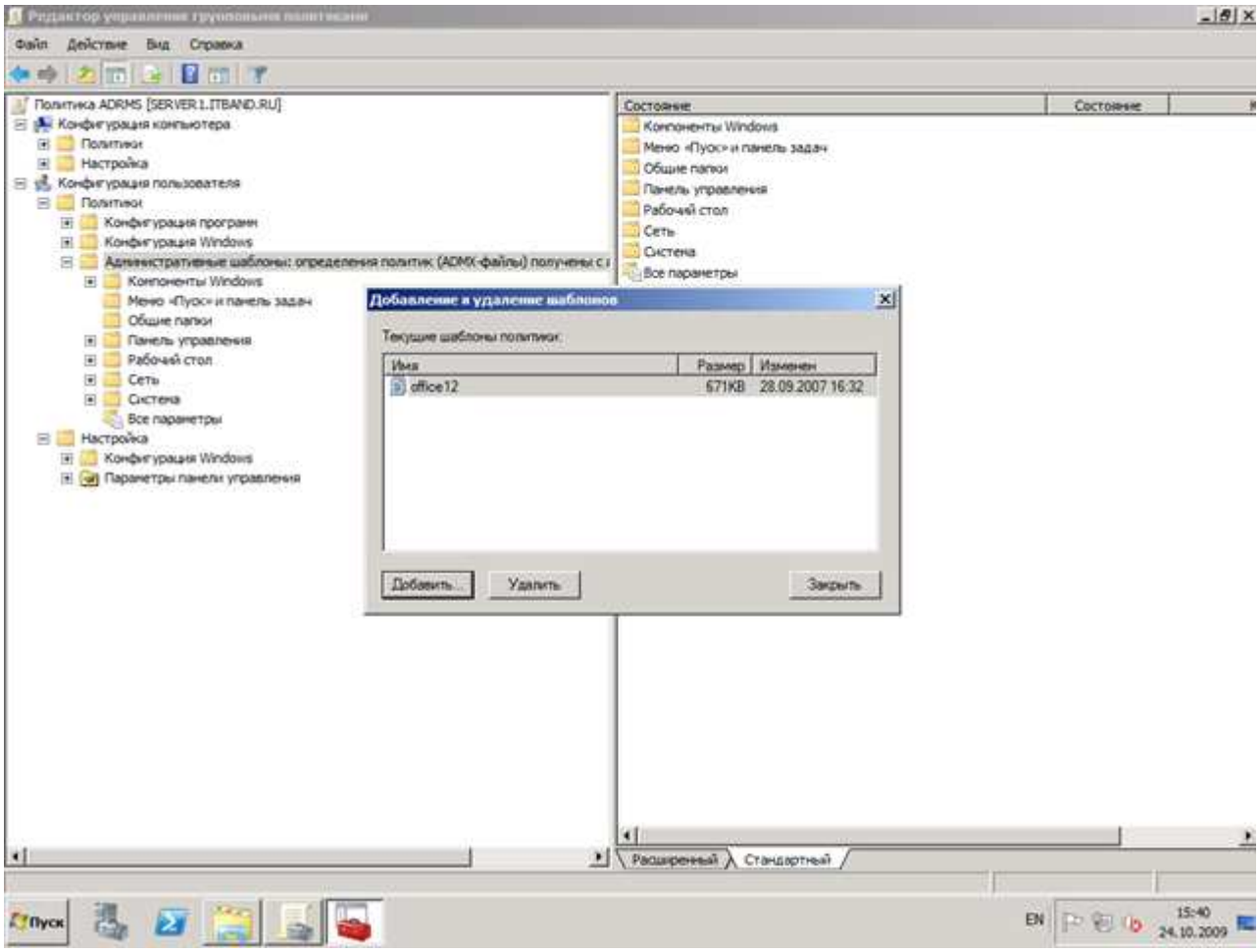


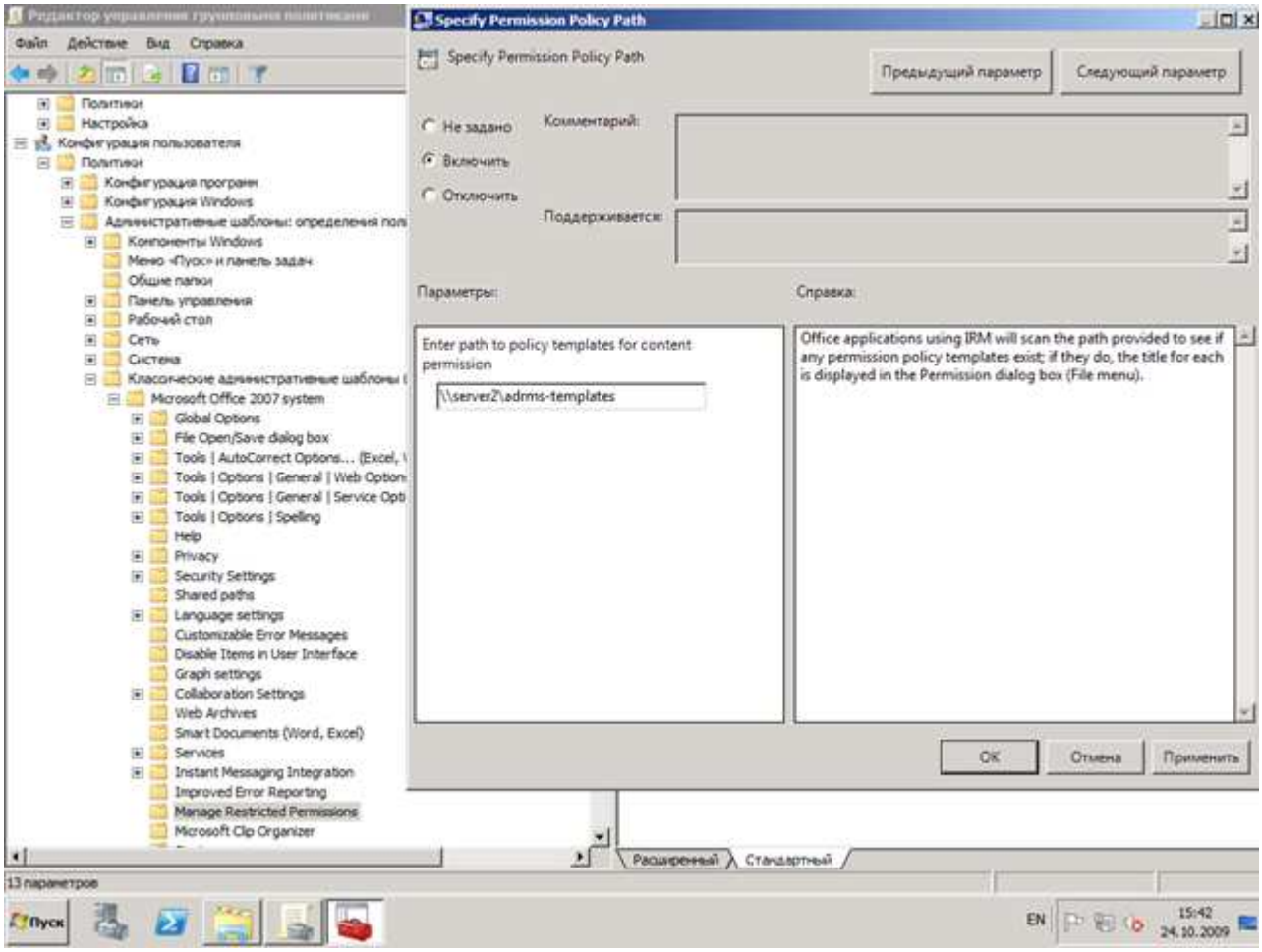
Поясню, установленные разрешения. Учетная запись, от имени которой работает служба AD RMS, должна иметь право «Изменение», чтобы при создании в оснастке «Active Directory Rights Management Services» нового шаблона он автоматически появлялся в папке «***adrms-templates***». Если мы дадим чтение всем пользователям, то любой желающий сможет защищать документы этим шаблоном. Поскольку мы точно знаем, что защищать будет пользователь ***Bgates,*** то и права

на папку даем ему. При желании можно настроить видимость будущих шаблонов более гибко, если использовать разрешения на XML-файлы шаблонов вместо папки.

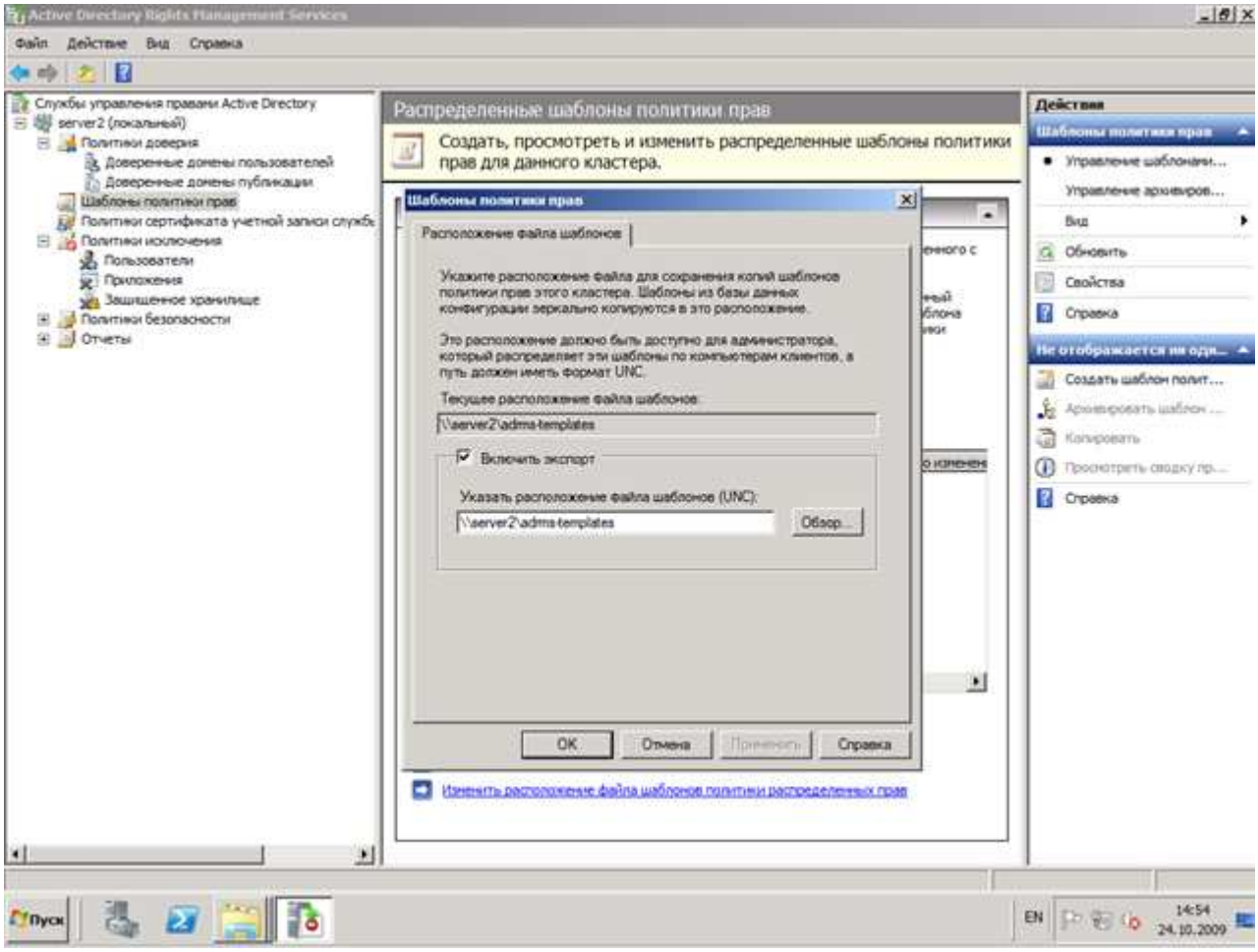
Папку, из которой будут распространяться шаблоны, мы создали, и теперь надо каким-то образом объяснить нашему пользователю ***Bgates*** откуда он должен брать шаблоны, в противном случае при попытке защитить документ, Microsoft Office 2007 их просто не увидит.

Указывать папку, хранящую шаблоны, мы будем с помощью групповой политики, но для этого нам понадобится административный шаблон управленияOffice 2007, который можно *скачать с сайта Microsoft*. Добавляем этот шаблон в уже созданную во второй части политику «***IE Security Zone***» и находим параметр «***Specify Permission Policy Path***».

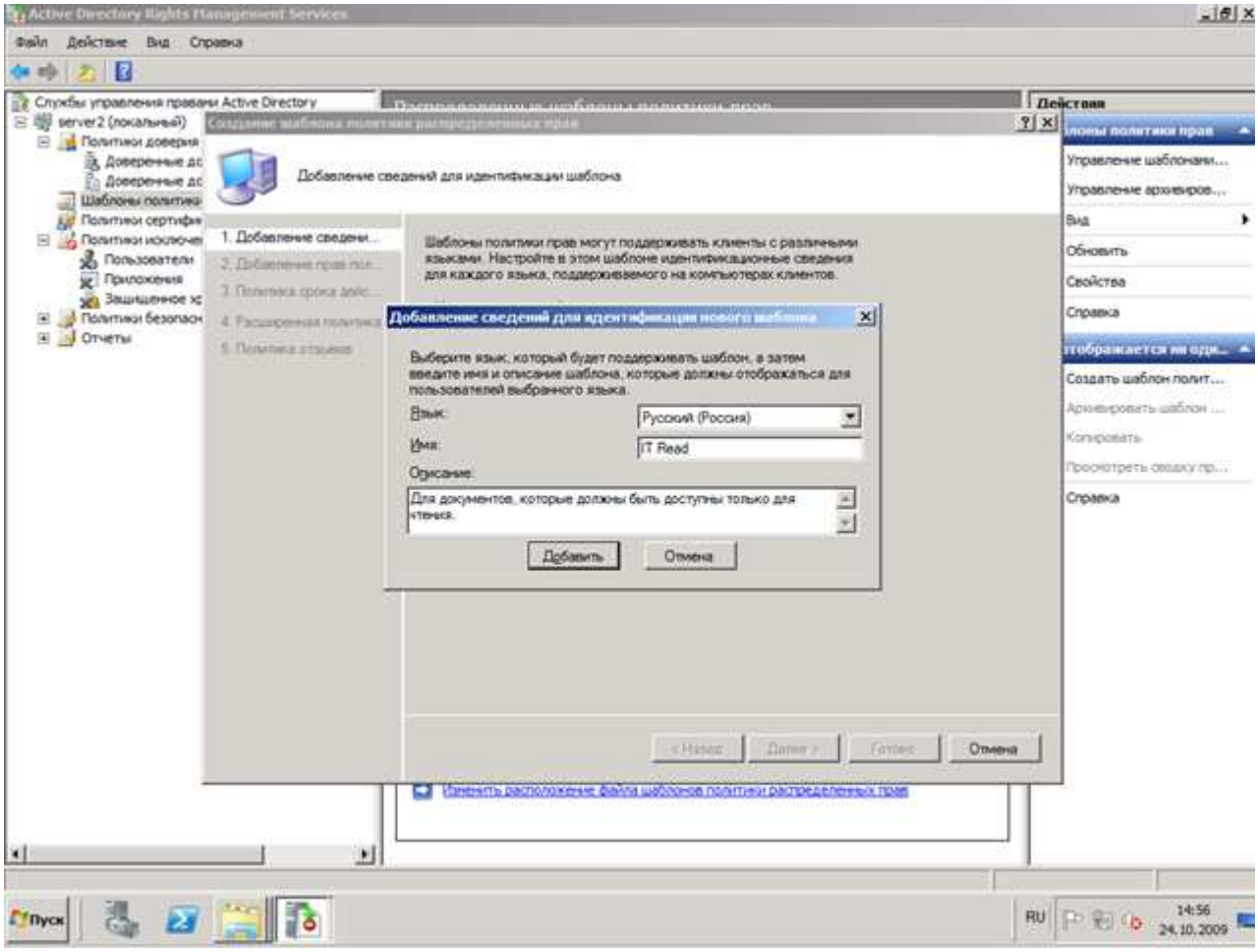




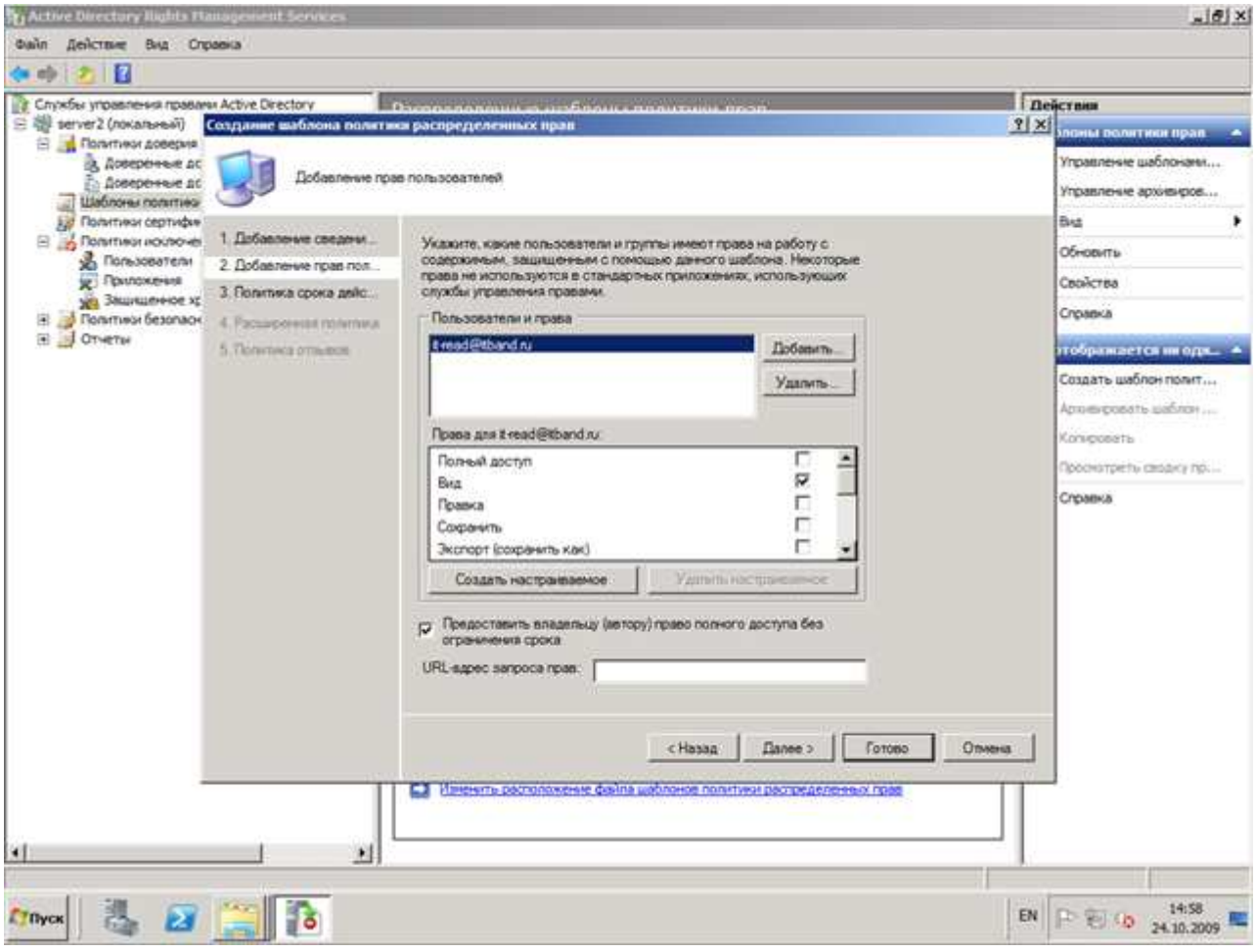
Включаем параметр «***Specify Permission Policy Path»*** и приписываем в нем путь к созданной в первой части статьи папке, будущем хранилище шаблонов. Напомню, что политика в который мы производим данные манипуляции была создана ранее и применяется ко всем пользователям ИТ-отдела.При этом она также добавляет адрес нашего сервера AD RMS в местную интрасеть Internet Explorer.



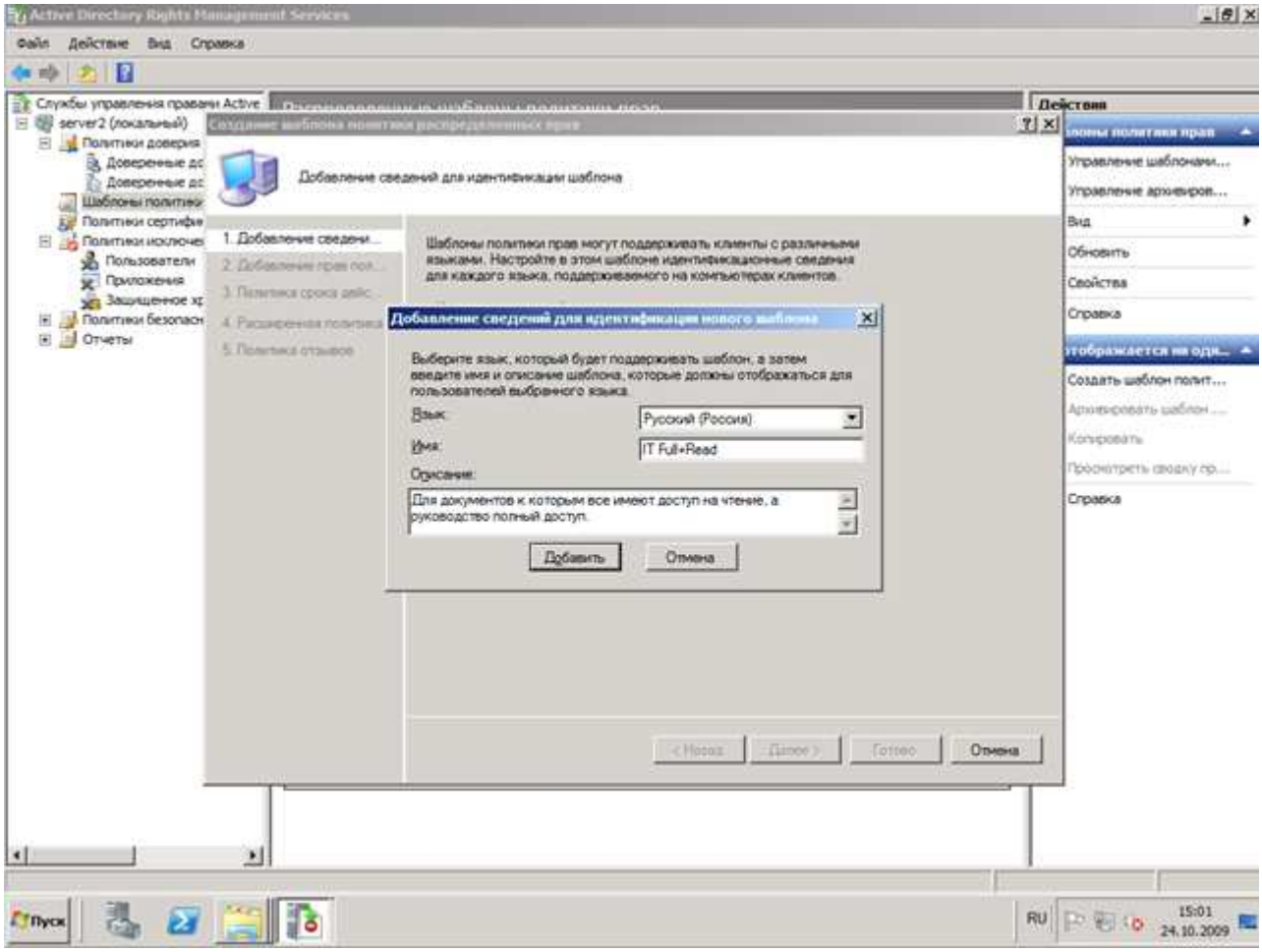
Открываем оснастку ***«Active Directory Rights Management Services»*** и разворачиваем ***«Шаблоны политики прав».*** Сразу говорим, куда наш RMS-сервер должен сохранять копии будущих шаблонов, т.е. включаем экспорт и прописываем сетевой путь к нашей папке. Теперь все готово создания самих шаблонов.



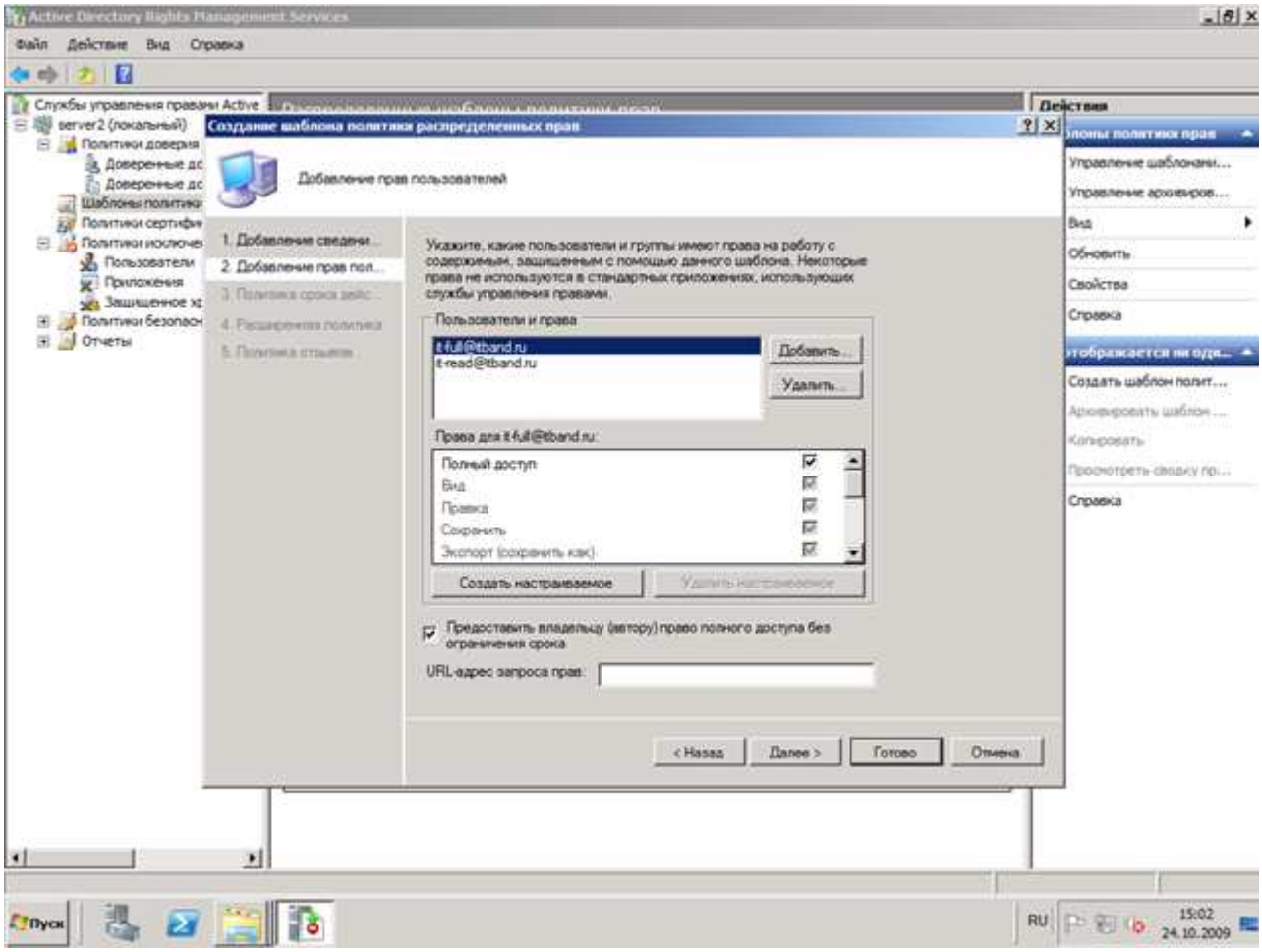
Там же в разделе ***«Шаблоны политики прав»***выбираем «***Создание шаблона политики распределенных прав***» и запускаем мастер. В нем прописываем имя и назначения шаблона. По картинке видно, что этот шаблон прав будет давать разрешение на чтение. Нажимаем «Далее».



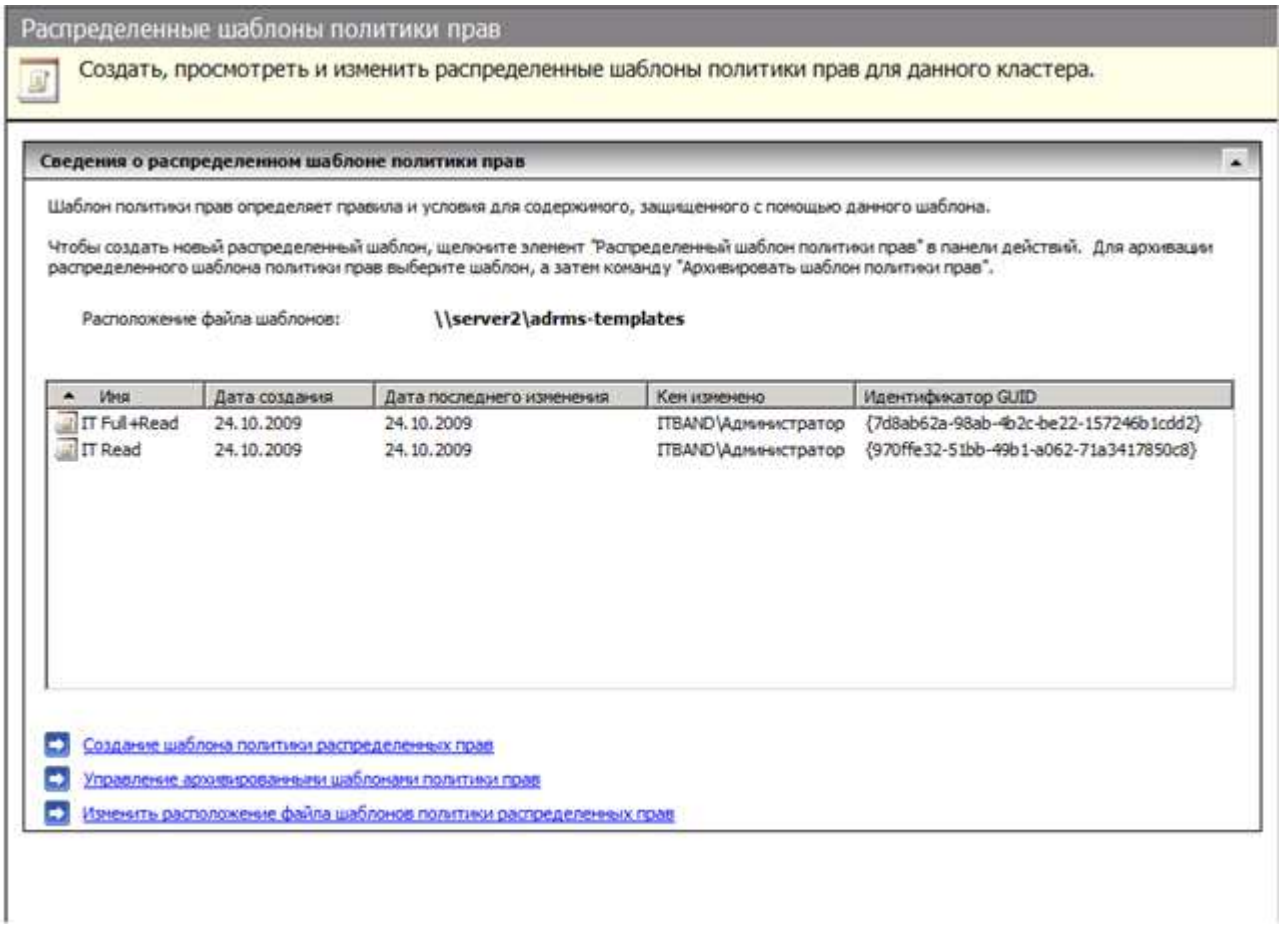
На следующем окне указываем, что право будет даваться группе «***it-read***». Эта группа имеет адрес электронной почты(обязательное условие), а ее членами являются все сотрудники ИТ-отдела. Из всевозможных прав устанавливаем только одну галочку «***Вид***». Нажимаем «Готово» и получаем первый созданный шаблон.



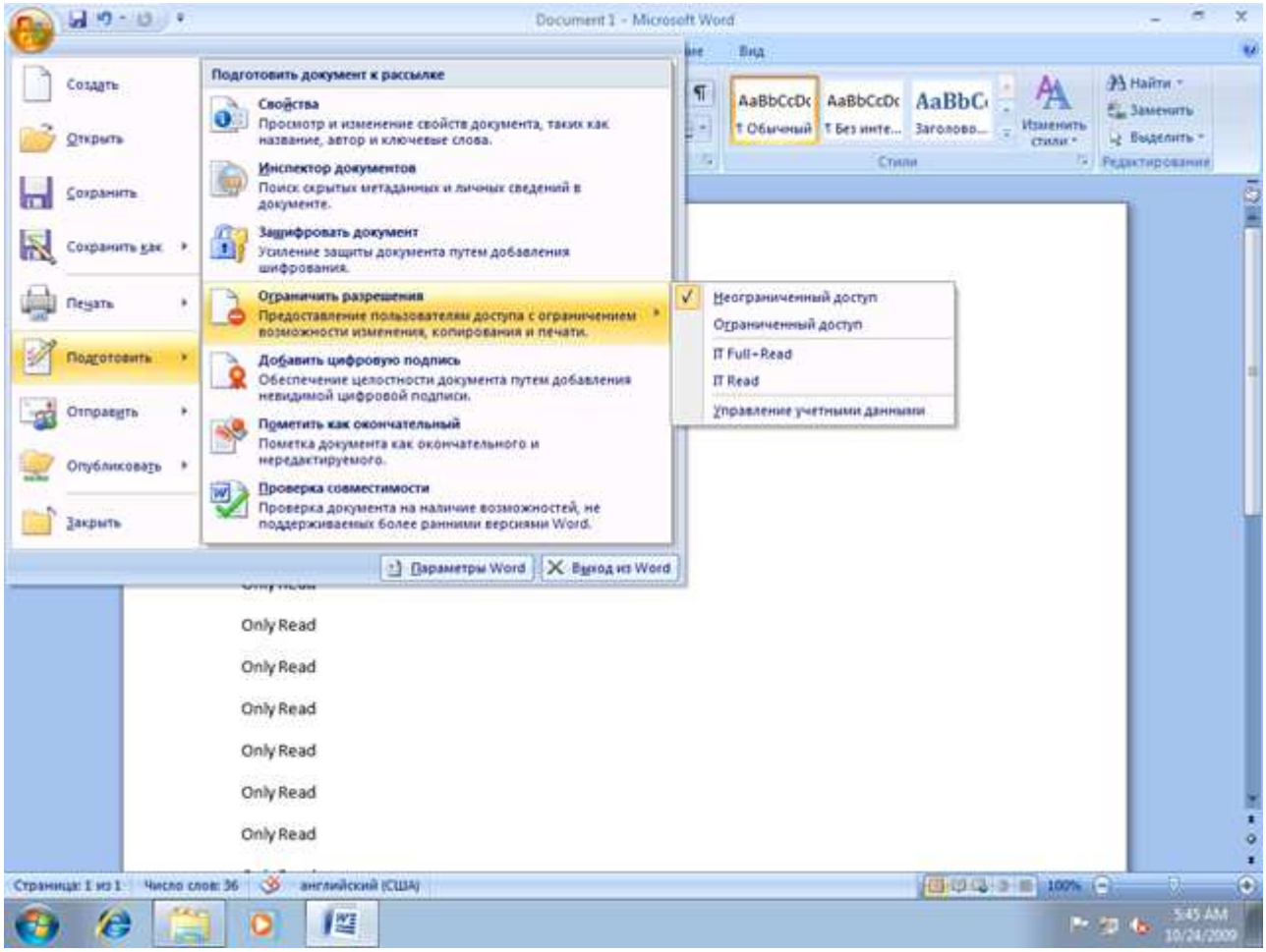
Теперь для создания второго шаблона повторяем процедуру запуска мастера. Указываем имя шаблона «***IT Full-Read***» и краткое описание. Нажимаем«Далее».



Права второго шаблона несколько сложней. Мы также даем группе «***it-read***» право «***Вид***», а второй строчкой добавляем группу «***it-full***» и присваиваем ей права «***Полный доступ***». А значит, все документы, к которым будет применен этот шаблон, пользователь ***sbalmer*** сможет редактировать, сохранять и.т.д. Но самое главное он сможет снимать защиту,сделанную с помощью этого шаблона.



После всех этих манипуляций вы увидите приблизительно такую картину: два шаблона, даты создания и последнего изменения, а также путь, по которому они хранятся.



Остается проверить работу шаблона в действии. Теперь при попытке пользователя ***Bgates*** защитить документ, ему будет предоставлено два шаблона на выбор «***IT Full + Read***» и «***IT Read***». Остальные сотрудники отдела, естественно, эти шаблоны видеть не будут, что никак не помешает им работать с документами, которые этими шаблонами защищены.

Теперь сделаем несколько выводов:

1. Если не задано обратное, человек защитивший документ с помощью AD RMS всегда имеет к нему неограниченный доступ. При этом неважно, кто был автором этого документа и владельцем.

2. Если пользователь входит в несколько групп и каждой группе даны свои права, то в результате сотрудник получит результирующие разрешения. Хороший пример ***sbalmer***,он состоит в обеих группах, по одной получает чтение, по другой полный доступ.В результате при шаблоне «***IT Full + Read***» он работает с полным доступом.

3. Право «***Полный доступ***» дает возможность снять защиту с документа, поэтому использовать его нужно очень осторожно, для полной свободы в редактировании файла «***Полный доступ***» не нужен.

Надеюсь, в общих чертах с шаблонами вы познакомились и при необходимости сможете их настроить. В следующей части поговорим о такой роли как «***супер-пользователь***» и других возможностях AD RMS.