МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Воронежский государственный технический университет»

Кафедра экономики и управления на предприятии машиностроения

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к проведению лабораторных работ по дисциплине «Оценка рисков» для студентов специальности 38.05.01 «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ» (всех форм обучения)

Воронеж 2018

УДК 330.131.7:338.24:336.767.2
ББК 65.9(2)26
Е25

Составители: д-р экон. наук, проф. Е.П. Енина;
канд. экон. наук, доц. И.А. Шишкин

Методические указания к проведению лабораторных работ по дисциплине «Оценка рисков» для студентов специальности 38.05.01 «Экономическая безопасность»/ ФГБОУ ВО «Воронежский государственный технический университет»; сост.: Е.П. Енина, И.А. Шишкин. – Воронеж: ВГТУ, 2018. 58с.

В методических указаниях содержатся материалы, которые позволят студентам подготовиться к выполнению лабораторных работ по дисциплине «Оценка рисков». Издание соответствует требованиям Государственного образовательного стандарта высшего профессионального образования 38.05.01 по специальности «Экономическая безопасность» специализации «Экономика и организация производства на режимных объектах».

Методические указания предназначены для студентов экономических специальностей очной и заочной форм обучения.

Табл.16 Рис.60 Библиогр. 4 названия.

Научный редактор: д-р экон. наук, проф. О.Г.Туровец.

Рецензент: д-р экон. наук, проф. И.В.Каблашова.

Печатается по решению учебно-методического совета Воронежского государственного технического университета

ОГЛАВЛЕНИЕ

Введение

В результате освоения дисциплины «Оценка рисков»обучающийся должен:

Знать:

– основные угрозы экономической безопасности (ПК-32);

– экспертные оценки факторов риска (ПК-40);

– управленческие решения с учетом критериев рисков (ПК-43).

Уметь:

– проводить анализ и давать оценку возможным экономическим рискам на основе прогнозов динамики основных социально-экономических показателей деятельности хозяйствующих субъектов (ПК-36);

– осуществлять экспертную оценку факторов риска (ПК-40);

– проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32);

–принимать оптимальные управленческие решения (ПК-43).

Владеть:

– способностью принимать оптимальные управленческие решения с учетом критерия рисков и возможности использования имеющихся ресурсов (ПК-43);

–способностью составлять прогнозы динамики основных экономических и социально-экономических показателей деятельности хозяйствующих субъектов (ПК-36);

– способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32).

ЛАБОРАТОРНАЯ РАБОТА №1
Количественные характеристики и схемы оценки рисков в условиях неопределенности

Матрицы последствий и матрицы рисков.

Понятие риска предполагает наличие рискующего; будем называть его Лицом, Принимающим Решения (ЛПР).

Допустим, рассматривается вопрос о проведении финансовой операции в условиях неопределенности. При этом у ЛПР есть несколько возможных решений $i = 1,2,...,m$, а реальная ситуация неопределенна и может принимать один из вариантов$j = 1,2,..., n$. Пусть известно, что если ЛПР примет i-е решение, а ситуация примет j-ый вариант, то будет получен доход q_{ij}. Матрица $Q = (q_{ij})$ называется ***матрицей последствий*** (возможных решений).

Оценим размеры риска в данной схеме.

Пусть принимается i-е решение. Очевидно, если бы было известно, что реальная ситуация будет j-я, то ЛПР принял бы решение, дающее доход $q_j = \max\limits_i q_{ij}$. Однако, i-е решение принимается в условиях неопределенности. Значит, ЛПР рискует получить не q_j , а только q_{ij}. Таким образом, существует реальная возможность недополучить доход, и этому неблагоприятному исходу можно сопоставить рискr_{ij}, размер которого целесообразно оценить как разность

$r_{ij}=q_j - q_{ij}$. (1)

Матрица $R = (r_{ij})$ называется ***матрицей рисков***.

Используя формулу (1), составим матрицу рисков

$R = (r_{ij})$ по заданной матрице последствий

$$Q = \begin{pmatrix} 5 & 2 & 8 & 4 \\ 2 & 3 & 4 & 12 \\ 8 & 5 & 3 & 10 \\ 1 & 4 & 2 & 8 \end{pmatrix}.$$

Решение. Очевидно, $q_1 = \max\limits_i q_{i1} = 8$; аналогично $q_2 = 5$, $q_3 = 8$, $q_4 = 12$. Следовательно, матрица рисков имеет вид

$$R = \begin{pmatrix} 3 & 3 & 0 & 8 \\ 6 & 2 & 4 & 0 \\ 0 & 0 & 5 & 2 \\ 7 & 1 & 6 & 4 \end{pmatrix}.$$

Анализ связанной группы решений в условиях полнойнеопределенности

Полная неопределенность означает отсутствие информации о вероятностных состояниях среды (“природы”), например, о вероятностях тех или иных вариантов реальной ситуации; в лучшем случае известны диапазоны значений рассматриваемых величин. Рекомендации по принятию решений в таких ситуациях сформулированы в виде определенных правил (критериев). Рассмотрим основные из них.

Критерий (правило) максимакса. По этому критерию определяется вариант решения, максимизирующий максимальные выигрыши - например, доходы – для каждого варианта ситуации. Это критерий ***крайнего (“розового”) оптимизма***, по которому наилучшим является решение, дающее максимальный выигрыш, равный $\max\limits_i \left(\max\limits_j q_{ij} \right)$.

Рассматривая *i*-е решение, предполагают самую хорошую ситуацию, приносящую доход $a_i = \max_j q_{ij}$, а затем выбирают решение с наибольшим a_i.

Для матрицы последствий необходимо выбрать вариант решения по критерию максимакса.

Решение. Находим последовательность значений $a_i = \max_j q_{ij}$: $a_1=8$, $a_2=12$, $a_3=10$, $a_4=8$. Из этих значение находим наибольшее: $a_2=12$. Следовательно, критерий максимакса рекомендует принять второе решение ($i=2$).

Правило Вальда (правило максимина, или критерий крайнего пессимизма). Рассматривая i-е решение, будем полагать, что на самом деле ситуация складывается самая плохая, т.е. приносящая самый малый доход: $b_i=\min q_{ij}$. Но теперь выберем решение i_0 с наибольшим b_{i_0}. Итак, правило Вальда рекомендует принять решениеi_0 такое, что $b_{i_0} = \max_i b_i = \max_i \left(\min_j q_{ij} \right)$.

Для матрицы последствий необходимо выбрать вариант решения по критерию Вальда.

Решение. Имеем $b_1= 2$, $b_2 = 2$, $b_3 = 3$, $b_4 = 1$. Теперь из этих значений выбираем максимальное $b_3 = 3$. Значит, правило Вальда рекомендует принять 3-е решение ($i=3$).

Правило Сэвиджа (критерий минимаксного риска). Этот критерий аналогичен предыдущему критерию Вальда, но ЛПР принимает решение, руководствуясь не матрицей последствий Q, а матрицей рисков R = (r_{ij}). По этому критерию лучшим является решение, при котором максимальное значение риска будет наименьшим, т.е. равным $\min_i \left(\max_j r_{ij} \right)$. Рассматривая i-е решение, предполагают ситуацию максимального риска $r_i= \max_j r_{ij}$ и выбирают вариант решения i_0 с наименьшим $r_{i_0} = \min_i b_i = \min_i \left(\max_j r_{ij} \right)$.

Для исходных данных необходимо выбрать вариант решения в соответствии с критерием Сэвиджа.

Решение. Рассматривая матрицу рисков R, находим последовательность величин $r_i = \max_j r_{ij}$: $r_1 = 8, r_2 = 6, r_3 = 5$, $r_4 = 7$. Из этих величин выбираем наименьшую: $r_3 = 5$. Значит, правило Сэвиджа рекомендует принять 3-е решение ($i=3$). Заметит, что это совпадает с выбором по критерию Вальда.

Правило Гурвица (взвешивающее пессимистический и оптимистический подходы к ситуации). По данному критерию выбирается вариант решения, при котором достигается максимум выражения $c_i= \{\lambda \min q_{ij} + (1 - \lambda) \max q_{ij}\}$, где $0 \le \lambda \le 1$. Таким образом, этот критерий рекомендует руководствоваться некоторым средним результатом *между крайним оптимизмом и крайним пессимизмом*. При $\lambda=0$ критерий Гурвица совпадает с максимаксным критерием, а при $\lambda=1$ он совпадает с критерием Вальда. Значение λ выбирается из субъективных (интуитивных) соображений.

Для матрицы последствий необходимо выбрать наилучший вариант решения на основе критерия Гурвица при $\lambda =1/2$.

Решение. Рассматривая матрицу последствий Q по строкам, для каждого i вычисляем значения $c_i= 1/2 \min q_{ij} + 1/2 \max q_{ij}$. Например, $c_1=1/2*2+1/2*8=5$; аналогично находятся $c_2=7$; $c_3=6,5$; $c_4= 4,5$. Наибольшим является $c_2=7$. Следовательно, критерий Гурвица при заданном $\lambda =1/2$ рекомендует выбрать второй вариант ($i=2$).

Анализ связанной группы решений в условиях частичнойнеопределенности

Если при принятии решения ЛПР известны вероятности p_j того, что реальная ситуация может развиваться по варианту j, то говорят, что ЛПР находится в условиях частичной неопределенности. В этом случае можно руководствоваться одним из следующих критериев (правил).

Критерий (правило) максимизации среднего ожидаемого дохода. Этот критерий называется также **критерием максимума среднего выигрыша.**Если известны вероятности p_j вариантов развития реальной ситуации, то доход, получаемый при i-ом решении, является случайной величиной Q_i с рядом распределения

q_{i1}	q_{i2}	…	q_{in}
p_1	p_2	…	p_n

Математическое ожидание $M[Q_i]$ случайной величины Q_i и есть средний ожидаемый доход, обозначаемый также $\overline{Q_i}$:

$$\overline{Q_i} = M[Q_i] = \sum_{j=1}^{n} p_j q_{ij} .$$

Для каждого i-го варианта решения рассчитываются величины $\overline{Q_i}$, и в соответствии с рассматриваемым критерием выбирается вариант, для которого достигается $\max_i \overline{Q_i} = \max_i \sum_{j=1}^{n} p_j q_{ij}$

Пусть для исходных данных известны вероятности развития реальной ситуации по каждому из четырех вариантов, образующих полную группу событий:

p_1 =1/2, p_2=1/6, p_3=1/6, p_4=1/6. Выяснить, при каком варианте решения достигается наибольший средний доход и какова величина этого дохода.

Решение. Найдем для каждого i-го варианта решения средний ожидаемый доход: $\overline{Q_1}$ =1/2*5+1/6*2+1/6*8+1/6*4= 29/6, $\overline{Q_2}$ = 25/6, $\overline{Q_3}$ = 7, $\overline{Q_4}$ = 17/6. Максимальный средний ожидаемый доход равен 7 и соответствует третьему решению.

Правило минимизации среднего ожидаемого риска (другое название –**критерий минимума среднего проигрыша**).

В тех же условиях, что и в предыдущем случае, риск ЛПР при выборе i-го решения является случайной величиной R_i с рядом распределения

r_{i1}	r_{i2}	…	r_{in}
p_1	p_2	…	p_n

Математическое ожидание $M[R_i]$ и есть средний ожидаемый риск, обозначаемый также $\overline{R_i}$: $\overline{R_i}$ =$M[R_i]$= $\sum_{j=1}^{n} p_j r_{ij}$.. Правило рекомендует принять решение, влекущее минимальный средний ожидаемыйриск: $\min_i \overline{R_i} = \min_i \sum_{j=1}^{n} p_j r_{ij}$.

Исходные данные те же, необходимо определить, при каком варианте решения достигается наименьший средний ожидаемый риск, и найти величину минимального среднего ожидаемого риска (проигрыша).

Решение. Для каждого i-го варианта решения найдем величину среднего ожидаемого риска. На основе заданной матрицы риска R найдем: $\overline{R_1}$ = 1/2*3+1/6*3+1/6*0+1/6*8=20/6, $\overline{R_2}$ = 4, $\overline{R_3}$ = 7/6, $\overline{R_4}$ = 32/6.

Следовательно, минимальный средний ожидаемый риск равен 7/6 и соответствует третьему решению: $\min_i \overline{R_i} = \overline{R_i}$ = 7/6.

Оптимальность по Парето двухкритериальных финансовыхопераций в условиях неопределенности.

Из рассмотренного выше следует, что каждое решение (финансовая операция) имеет две характеристики, которые нуждаются в оптимизации: средний ожидаемый доход и средний ожидаемый риск. Таким образом, выбор наилучшего решения является оптимизационной двухкритериальной задачей. В задачах многокритериальной оптимизации основным понятием является понятие ***оптимальности по Парето***. Рассмотрим это понятие для финансовых операций с двумя указанными характеристиками.

Пусть каждая операция *a* имеет две числовые характеристики *E(a), r(a)* (например, эффективность и риск); при оптимизации *E* стремятся увеличить, а *r* уменьшить.

Существует несколько способов постановки таких оптимизационных задач. Рассмотрим такую задачу в общем виде. Пусть *A* — некоторое множество операций, и разные операции обязательно различаются хотя бы одной характеристикой. При выборе наилучшей операции желательно, чтобы *E* было больше, а r меньше.

Будем говорить, что операция ***адоминирует*** операцию *b,* и обозначать *a> b,* если *E(a)* ≥ *E(b)* и *r(a)* ≤*r(b)* и хотя бы одно из этих неравенств строгое. При этом операция *a* называется ***доминирующей***, а операция *b* – ***доминируемой***. Очевидно, что никакая доминируемая операция не может быть признана наилучшей. Следовательно, наилучшую операцию надо искать среди недоминируемых операций. Множество недоминируемых операций называется ***множеством (областью) Парето*** или ***множеством оптимальности по Парето***.

Для множества Парето справедливо утверждение: каждая из характеристик *E, r*является однозначной функцией другой, т.е. на множестве Парето по одной характеристике операции можно однозначно определить другую.

Для определения лучшей операции в ряде случаев можно применять некоторую *взвешивающую формулу,* в которую характеристики $\overline{R}$ и $\overline{Q}$ входят с определенными весами, и которая дает одно число, задающее лучшую операцию. Пусть, например, для операции *i* с характеристиками $(\overline{R}_i, \overline{Q}_i)$ взвешивающая формула имеет вид $f(i) = 3\overline{Q}_i - 2\overline{R}_i$, и наилучшая операция выбирается по максимуму величины *f(i)*. Эта взвешивающая формула означает, что ЛПР согласен на увеличение риска на три единицы, если доход операции увеличится при этом не менее, чем на две единицы. Таким образом, взвешивающая формула выражает отношение ЛПР к показателям дохода и риска.

Пусть исходные данные те же, т.е. для матриц последствий и риска известны вероятности вариантов развития реальной ситуации: $p_1 = 1/2$, $p_2 = 1/6$, $p_3 = 1/6$, $p_4 = 1/6$. В этих условиях ЛПР согласен на увеличение риска на две единицы, если при этом доход операции увеличится не менее, чем на одну единицу. Определить для этого случая наилучшую операцию.

Решение. Взвешивающая формула имеет вид $f(i) = 2\overline{Q}_i - \overline{R}_i$. Используя результаты расчетов, находим:

$f(1) = 2*29/6 - 20/6 = 6{,}33$; $f(2) = 2*25/6 - 4 = 4{,}33$;

$f(3) = 2*7 - 7/6 = 12{,}83$; $f(4) = 2*17/6 - 32/6 = 0{,}33$

Следовательно, лучшей является третья операция, а худшей – четвертая.

ЛАБОРАТОРНАЯ РАБОТА № 2
ИспользованиеMicrosoftSecurityAssessmentTool (MSAT)

Задание:

1. Ознакомиться с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT)/

Решение:

1. Как отмечают разработчики, приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности. В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

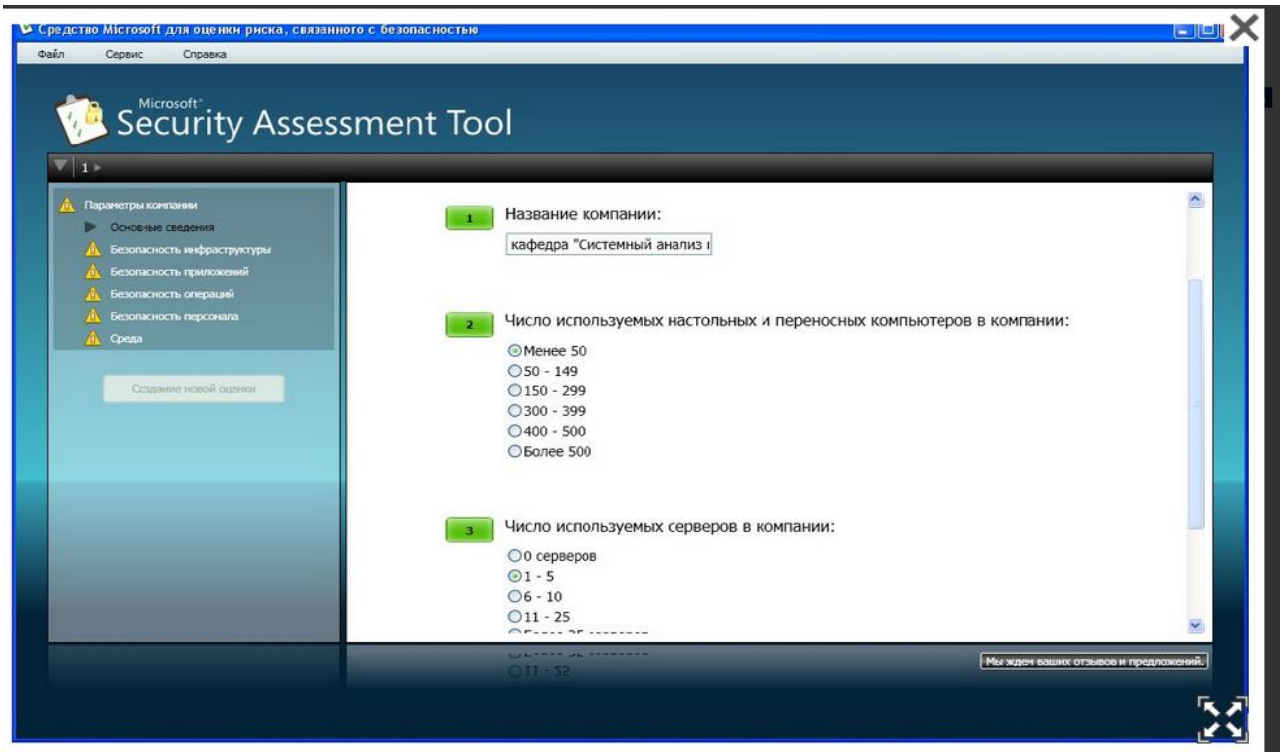


Рис. 1. Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая (рис. 1) касается общих сведений о компании – название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена "Безопасность инфраструктуры". Примеры вопросов – "использует ли компания подключение к Интернет", "размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте" и т.д. Остальные группы – "Безопасность приложений", "Безопасность операций", "Безопасность персонала", "Среда".

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты (рис. 2). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

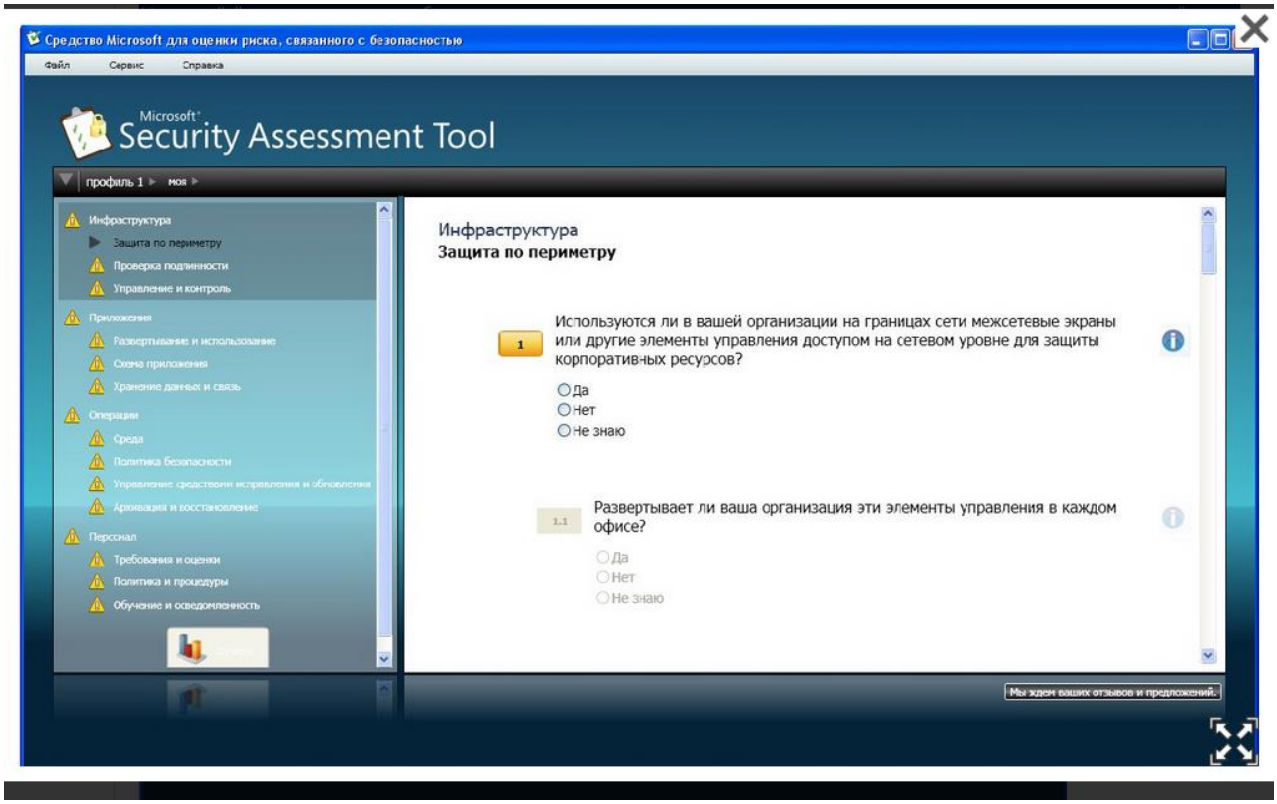


Рис. 2. Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет "Полный отчет". В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в табл. 1.

Таблица 1

Список предлагаемых действий

Список приоритетных действий	
Предмет анализа	Рекомендация
Высокий приоритет	
Операции >Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако, необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Вывод: В ходе данной лабораторной работы мы ознакомились с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью – Microsoft Security Assessment Tool (MSAT).

ЛАБОРАТОРНАЯ РАБОТА № 3
Использование цифровых сертификатов

Задание: ознакомиться с некоторыми вопросами использования цифровых сертификатов и рассмотреть возможности, которые предоставляет Windows Server 2008 по созданию собственно центра сертификации (Certification Authority - CA) на предприятии.

Ход работы:

Начнем с их использования протоколом SSL/TSL. Этот протокол широко применяется в сети Интернет для защиты данных передаваемых между web-серверами и браузером клиента. Для аутентификации сервера в нем используется сертификат X.509.

Для примера обратимся на сайт Ситибанка (http://www.citibank.ru), в раздел **"Мой банк"**, предназначенный для ведения банковских операций через Интернет (рис.3).

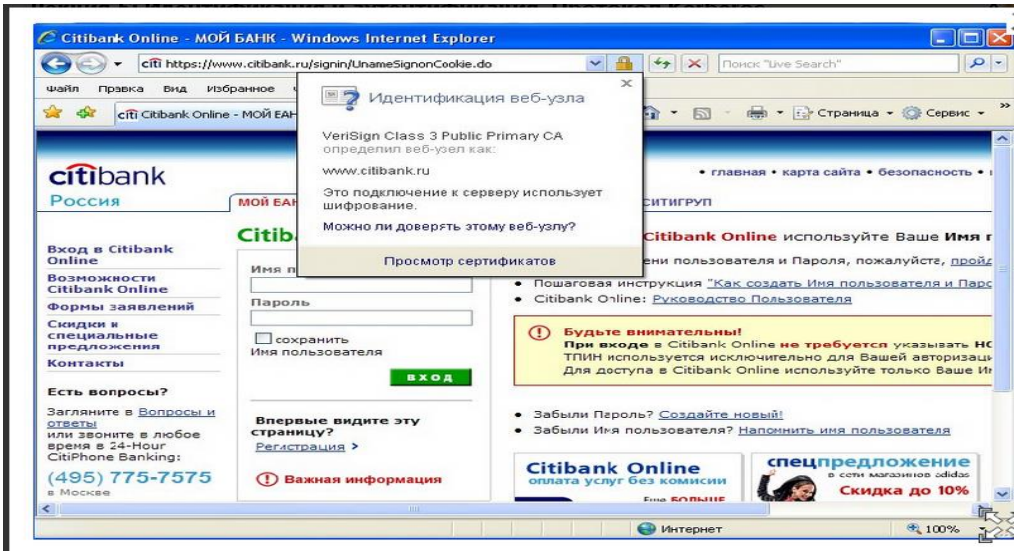


Рис. 3.Защищенное соединение

Выбрав "Просмотр сертификата" можно узнать подробности о получателе и издателе, другие параметры сертификата (рис. 4).

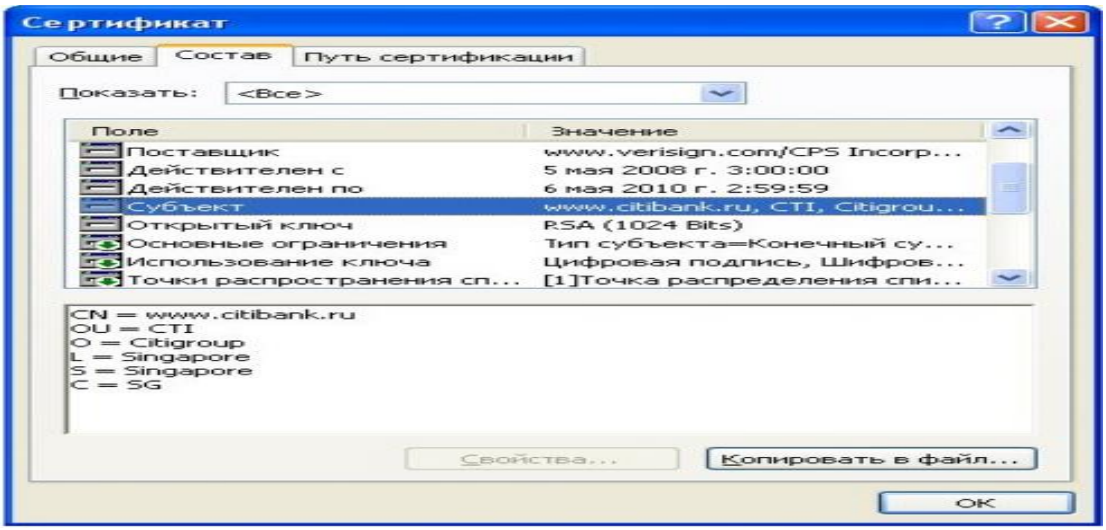


Рис. 4. Параметры сертификата

Посмотрим параметры сертификата "электронной сберкассы" Сбербанка - https://esk.sbrf.ru . Опишем, кем на какой срок и для какого субъекта сертификат был выдан.

Теперь рассмотрим другой вариант - мы подключаемся поSSL к web-серверу, а браузер не может проверить его подлинность. Подобная ситуация произошла при подключении в раздел Интернет-обслуживания Санкт-Петербургского филиала оператора мобильной связи Tele2 - https://www.selfcare.tele2.ru/work.html (на рис. 5).

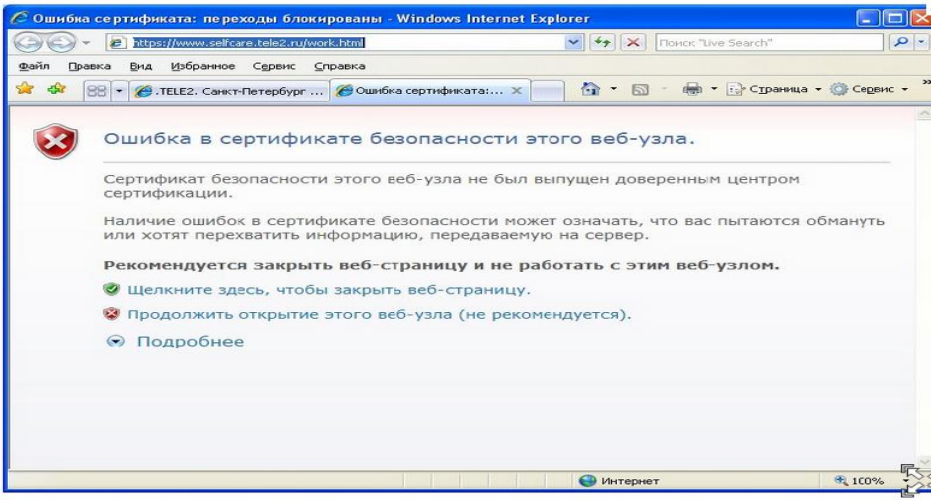


Рис. 5.Браузер сообщает о проблеме с сертификатом

Теперь рассмотрим, как хранятся сертификаты. Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC "Сертификаты".

Из меню Пуск —> Выполнить запустите консоль командой mmc. В меню Консоль выберите Добавить или удалить оснастку, а в списке оснасток выберите Сертификаты. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите пункт "Моей учетной записи".

Таким образом, мы можем просматривать сертификаты текущего пользователя. Если ранее сертификаты не запрашивались, то в разделе "Личные сертификаты" элементов не будет.

В разделе "Доверенные корневые центры сертификации" представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдемвнемсертификат VeriSign Class 3 Public Primary CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Теперь перейдем к разделу "Сертификаты, к которым нет доверия". Там находятся отозванные сертификаты. Как минимум, там будут находиться два сертификата, которые по ошибке или злому умыслу кто-то получил от имени корпорации Microsoft в центре сертификации VeriSing в 2001 году. Когда это выяснилось, сертификаты отозвали (рис. 6).

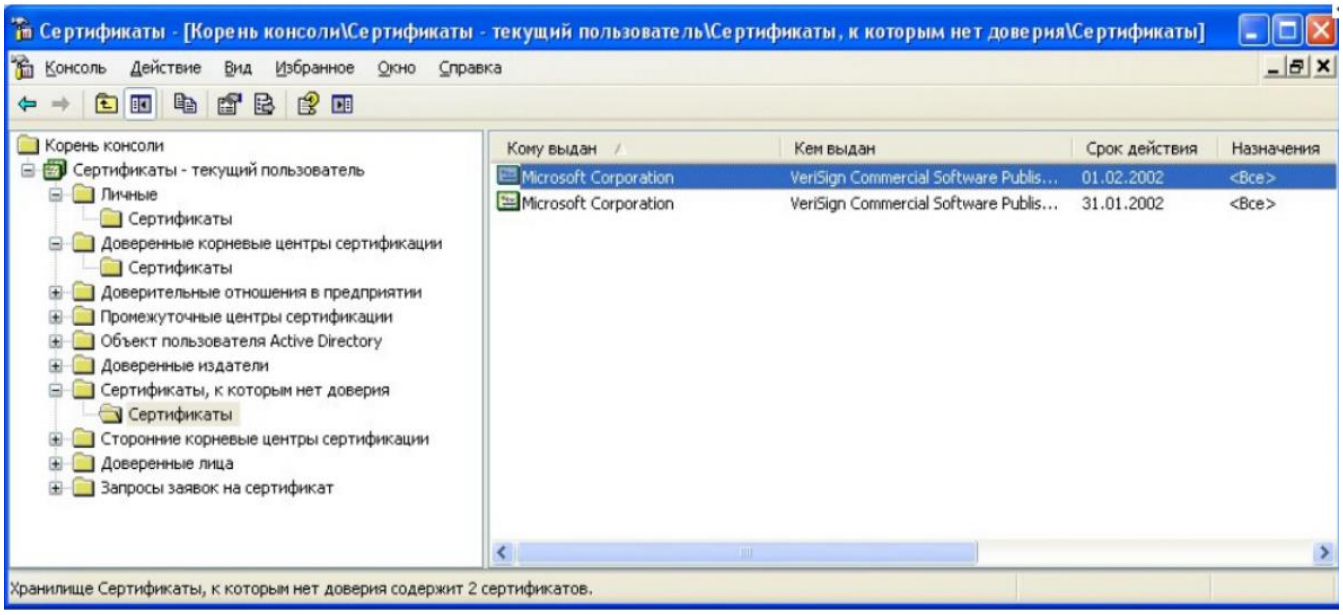


Рис. 6. Отозванные сертификаты

Теперь рассмотрим процесс запроса сертификата. На сайте центра сертификации Thawte http://www.thawte.com можно бесплатно получить сертификат для электронной почты. Дляэтоговменюсайта Products выберите Free Personal E-Mail Certificates. После этого надо заполнить небольшую анкету, указав имя, фамилию, страну, предпочитаемую кодировку, адрес электронной почты (должен быть обязательно действующим), дальше - пароль и контрольные вопросы для восстановления. Когда все заполнено, на указанный адрес почты будет отправлено письмо со ссылкой для выполнения дельнейших шагов генерации ключей и двумя проверочными значениями, которые нужно ввести, перейдя по ссылке. Таким образом, подлинность и принадлежность адреса будет подтверждена.

Далее система предложит ввести адрес почты (в качестве имя пользователя) и выбранный ранее пароль. После чего можно запросить сертификат X.509. Понадобится указать тип браузера и почтового клиента (например, Internet Explorer и Outlook). После этого потребуется ответить на запросы системы, касающиеся генерации ключей (разрешить выполнение ActiveX элемента, выбрать криптопровайдер, разрешить генерацию).

После завершения этого этапа на почтовый адрес будут выслано второе письмо, подтверждающее запрос сертификата. А спустя некоторое время - третье, со ссылкой для получения сертификата.

Пройдя по ссылке, надо будет снова ввести имя и пароль и на странице нажать кнопку "Install Your Cert" и согласиться с добавлением сертификата.

В результате в оснастке Сертификаты появится личный сертификат выпущенный издателем Thawte Personal Freemail Issuing CA для субъекта Thawte Freemail Member с указанным вами адресом почты (рис. 7).

Если использовать сертификат для защиты почты, дальнейшая настройка зависит от почтового клиента. Если это Microsoft Outlook, можно использовать встроенную в него поддержку протокола S/MIME. В Outlook 2003 для выбора сертификата надо войти в меню Сервис —> Параметры, там выбрать вкладку Безопасность и там в параметрах шифрованной электронной почты выбрать используемый сертификат и алгоритмы (рис. 8).

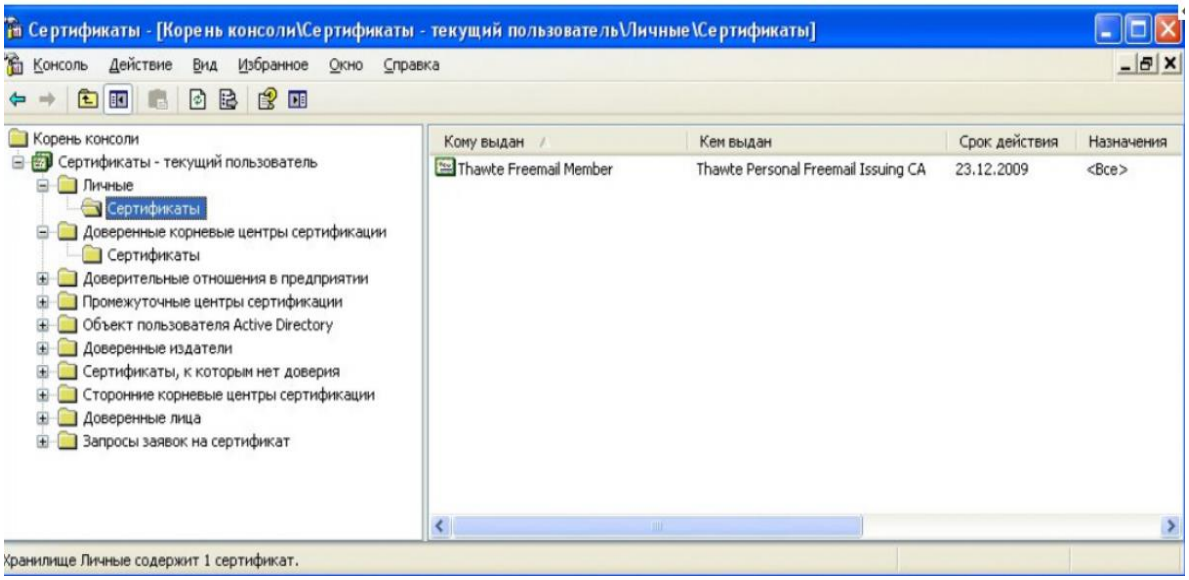


Рис. 7. Полученный сертификат

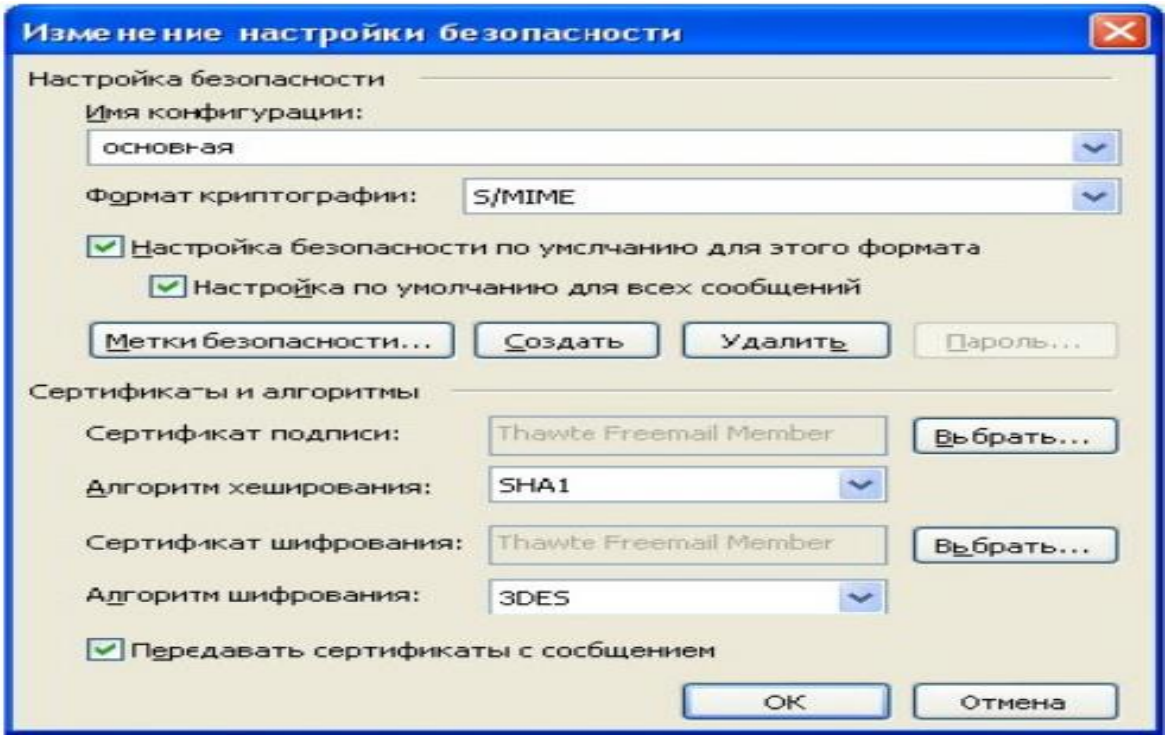


Рис.8.Выбор сертификата для защиты почты с помощью S/MIME в Outlook

В Windows Server 2008 для того, чтобы сервер смог работать как центр сертификации, требуется сначала добавить серверу роль Active Directory Certificate Services. Делается это помощью оснастки Server Manager, которую можно запустить из раздела Administrative Tools в стартовом меню.

В Server Manager раскроем список ролей и выберем добавление роли (Add Roles) – рис. 9.

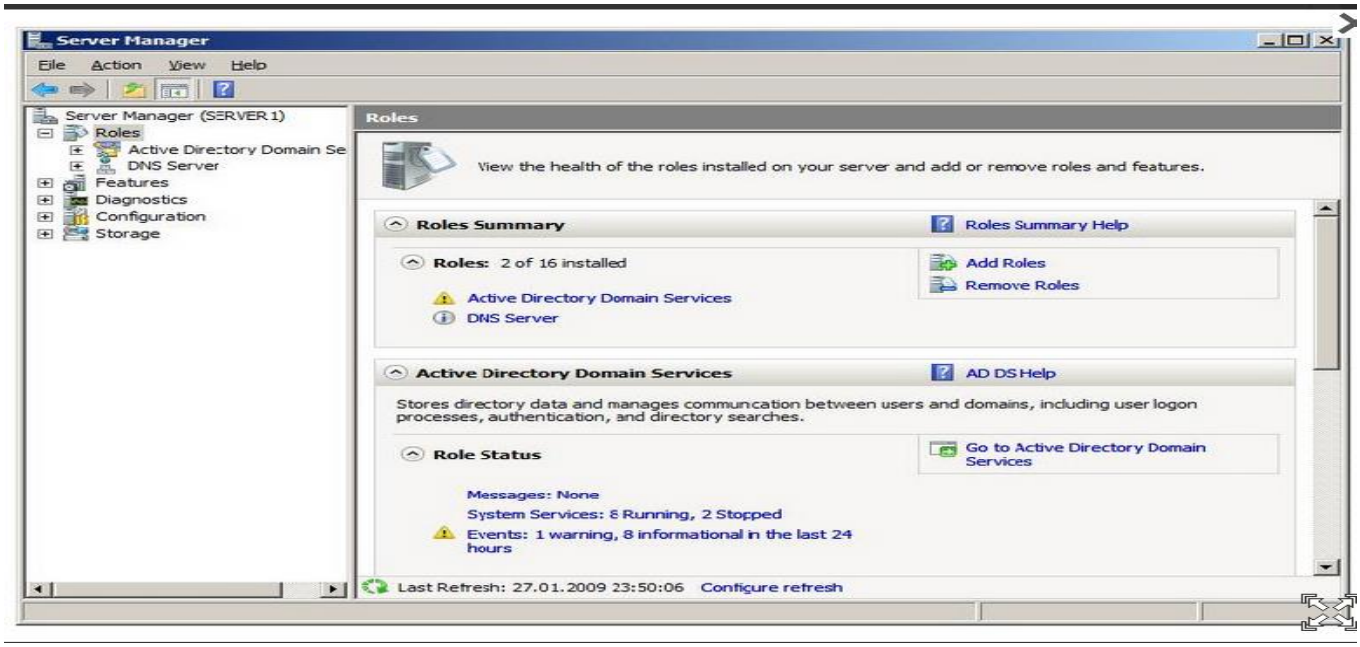


Рис. 9.Добавление роли

В списке доступных ролей выбираем требующуюся нам (Active Directory Certificate Services) и нажимаем Next (рис. 10). После этого запускается мастер, который сопровождает процесс установки.

В дополнение к обязательному компоненту "Certification Authority", могут быть установлены дополнительные средства, предоставляющие web-интерфейс для работы пользователей с CA (рис. 11). Это может понадобиться, например, для выдачи сертификатов удаленным или внешним, не зарегистрированным в домене, пользователям. Для выполнения данной лабораторной работы это не понадобится.

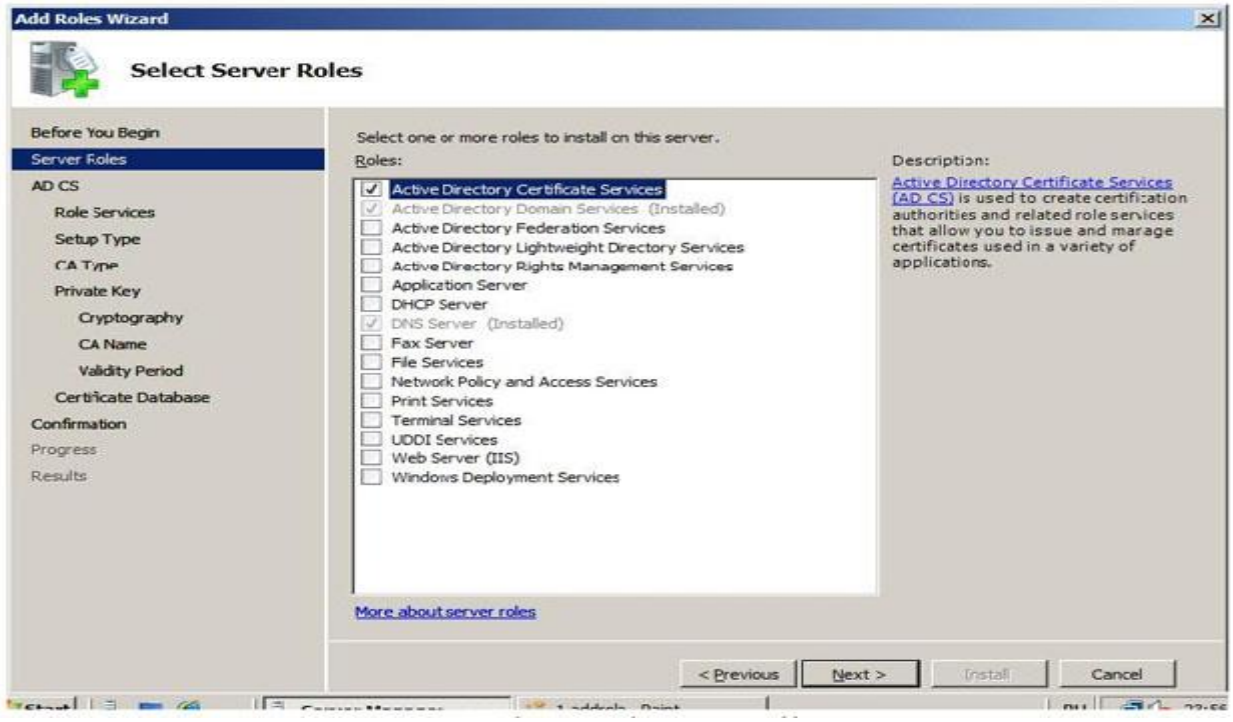


Рис. 10.Выбор добавляемой роли

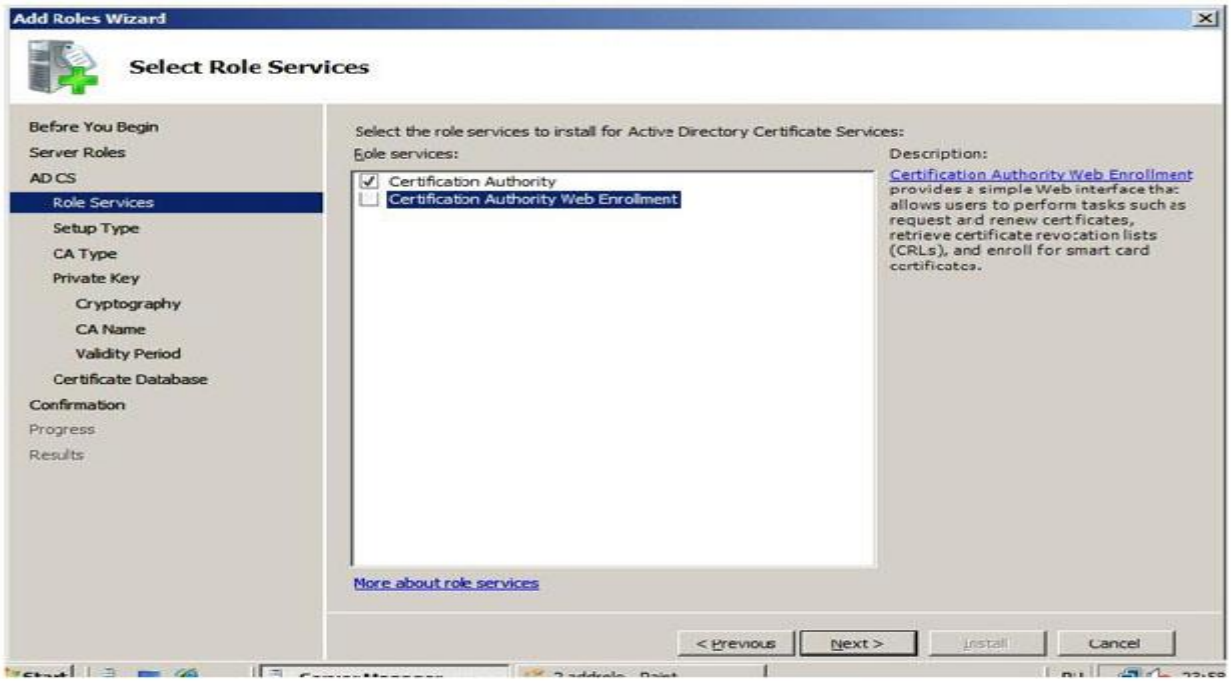


Рис. 11.Выбор устанавливаемых компонент

Следующий шаг – определения типа центра сертификации. Он может быть корпоративным (Enterprise) или отдельностоящим (Standalone) – рис. 12. Разница заключается в том, что EnterpriseCA может быть установлен только на сервер, являющийся членом домена, т.к. для его работы требуется служба каталога ActiveDirectory. Standalone CA может работать вне домена, например, обрабатывая запросы пользователей, полученные через web-интерфейс. Для выполнения лабораторной работы нужно выбрать версию Enterprise.

Следующее окно мастера позволяет определить, создается корневой (Root) или подчиненный (Subordinate) CA– рис. 13. В нашем примере создаваемый CA является первым и единственным, поэтому выбираем вариант Root.

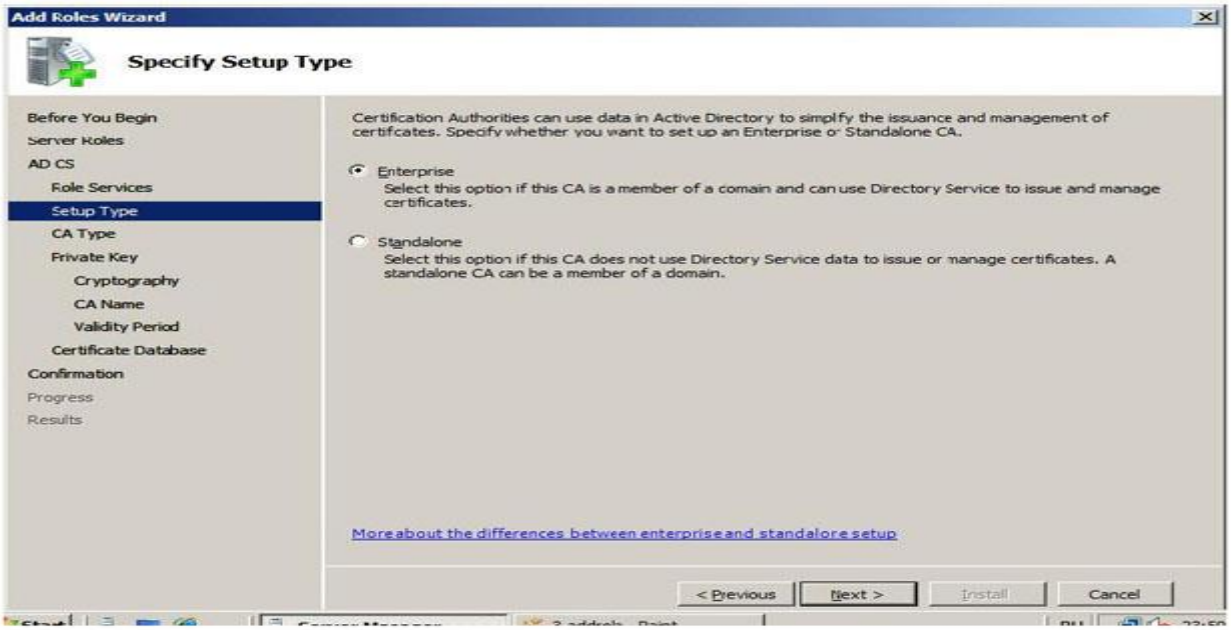


Рис. 12.(начало) Выбор типа центра сертификации

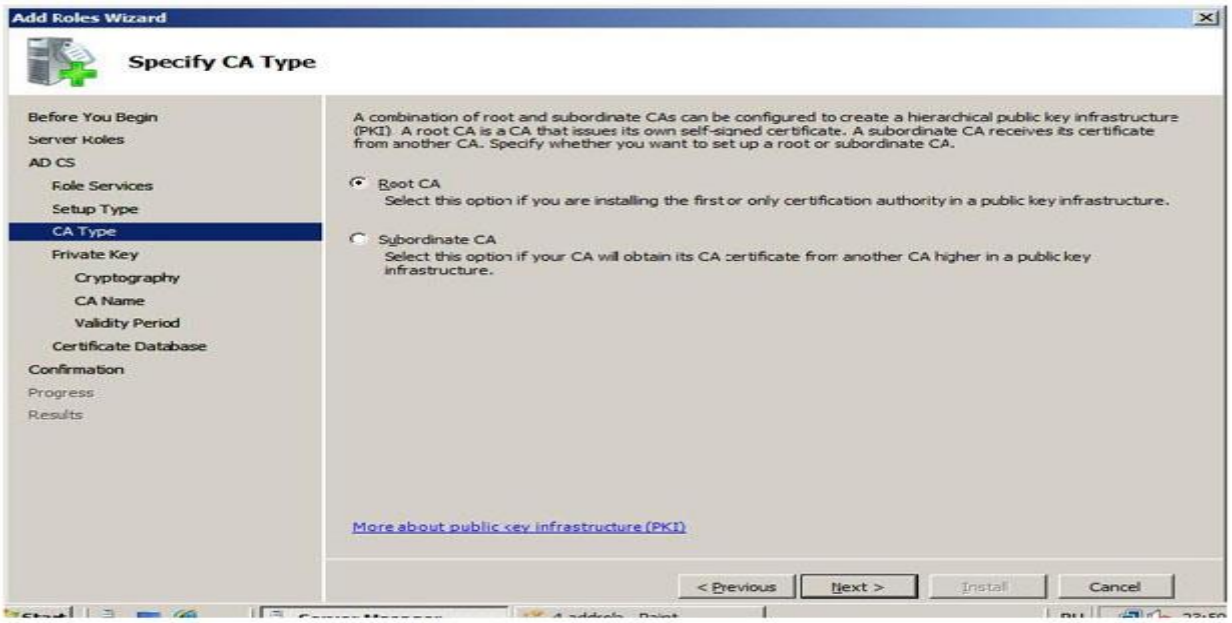


Рис. 12. (продолжение)Выбор типа центра сертификации

Создаваемый центр сертификации должен будет использовать при работе как минимум одну ключевую пару – открытый и секретный ключ (иначе он не сможет подписывать выпускаемые сертификаты). Создадим новый ключ. При этом, потребуется выбрать "криптографический провайдер" (программный модуль, реализующий крипто-алгоритмы) и алгоритм хеширования. Согласимся с настройками по умолчанию (рис. 13).

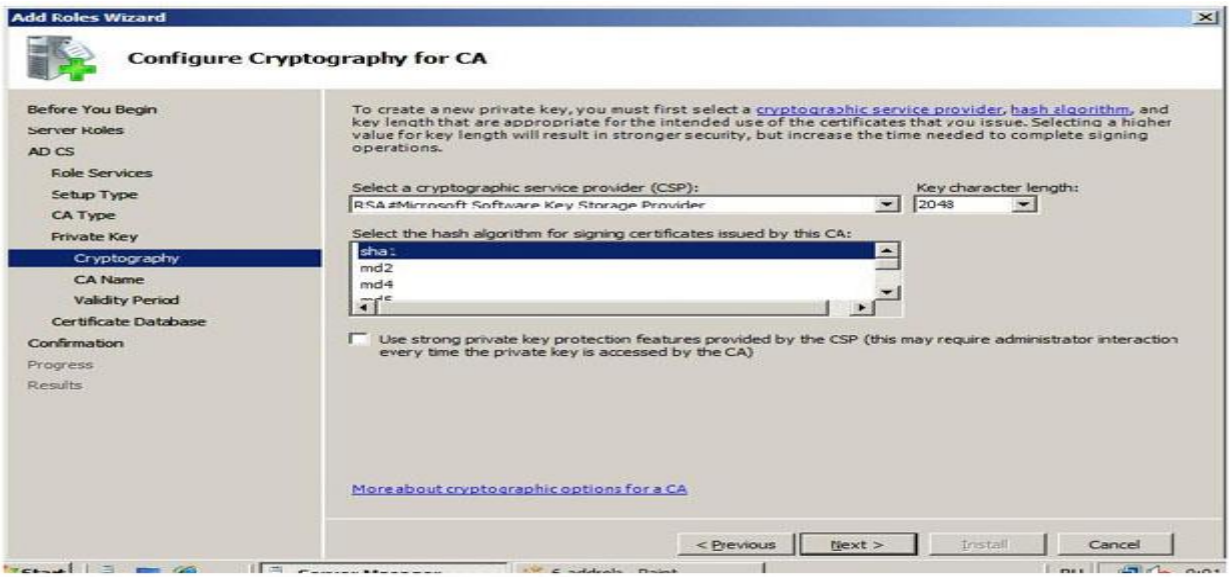


Рис. 13.Выбор криптографического провайдера и алгоритма хеширования

Далее потребуется указать имя CA, размещение базы сертификатов и лог-файлов, и подтвердить сделанные настройки. После этого, роль будет установлена.

На учебном сервере или виртуальной машине установите роль ActiveDirectoryCertificate Services с настройками, аналогичными рассмотренным выше.

Управлять работой CA можно из оснастки Certification Authority, которая должна появиться в разделе Administrative Tools (рис. 14).

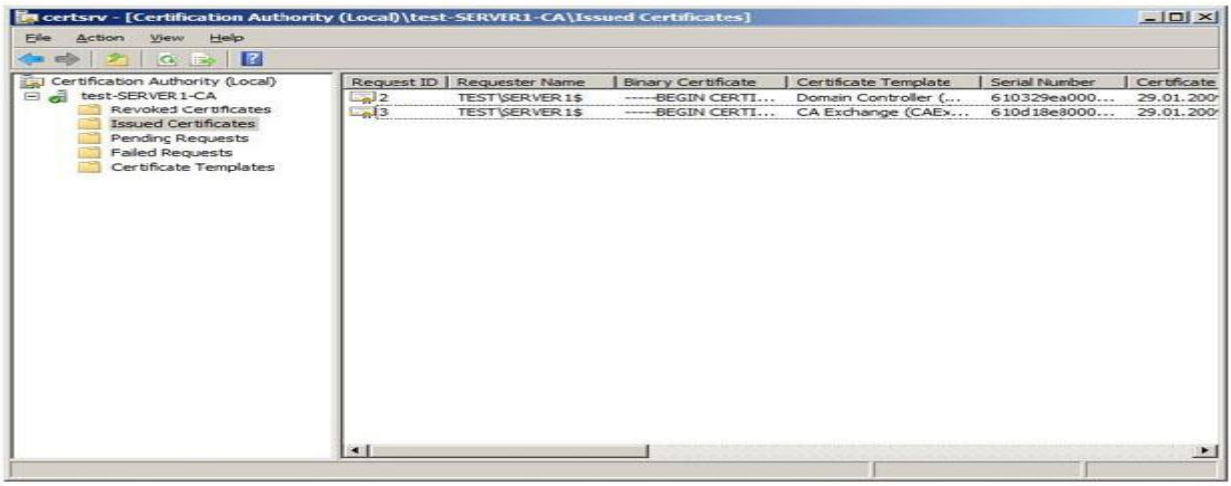


Рис. 14.Управление центром сертификации

Как видно на рисунке, только что установленный EnterpriseCA уже выпустил некоторое количество сертификатов для служебных целей (в частности, сертификаты контроллеров домена). В свойствах данного сервера (пунктProperties контекстного меню) можно посмотреть сделанные настройки. В частности, если выбрать закладку Policy Module и там нажать кнопку Properties, можно увидеть текущую настройку, определяющую порядок выдачи сертификатов (рис. 15).

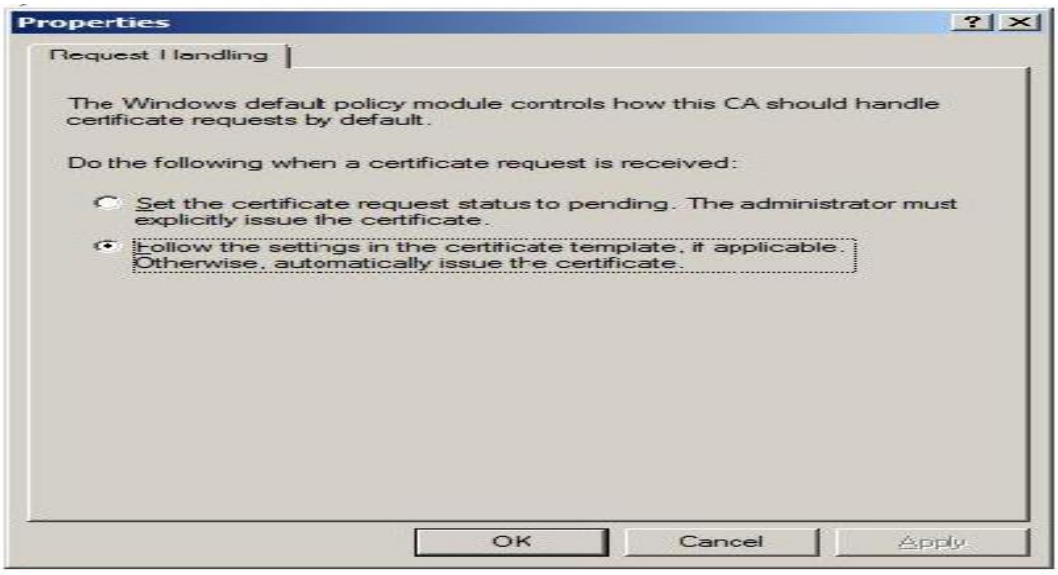


Рис. 15.Настройки, определяющие порядок выпуска сертификатов

В выбранном на рисунке случае, после запроса сертификат выдается в соответствии с настройками шаблона сертификата (или автоматически, если настроек нет). Возможен вариант, когда запрос помещается в очередь ожидающих, и сертификат выпускается только после утверждения администратором.

Ознакомимся с текущими настройками центра сертификации.

Опишем, какие шаблоны сертификатов (CertificateTemplates) определены и для каких целей служит каждый тип сертификатов.

Посмотрим, какие сертификаты выпущены (Issued Certificates), есть ли отозванные сертификаты (Revoked Certificates).

Теперь рассмотрим процесс получения цифрового сертификата. Сделать это можно с помощью оснастки Certificates, с которой мы познакомились в лабораторной № 6. Если она не установлена, запустите консольmmc и добавьте эту оснастку для текущей учетной записи.

Запустим оснастку, откроем раздел, посвященный сертификатам пользователя (Personal) и запросим сертификат (рис. 16). Из перечня предложенных шаблонов сертификатов выберем User. Данный тип сертификатов может использоваться для шифрования файлов с помощью EFS, защиты электронной почты и аутентификации пользователей.

Для пользователя будет сгенерирована ключевая пара, и на основе данных, взятых из базы службы ActiveDirectory и шаблона, будет выпущен сертификат, удостоверяющий открытый ключ.

Этот сертификат будет виден и в оснастке Certification Authority, в списке выпущенных данным сервером.

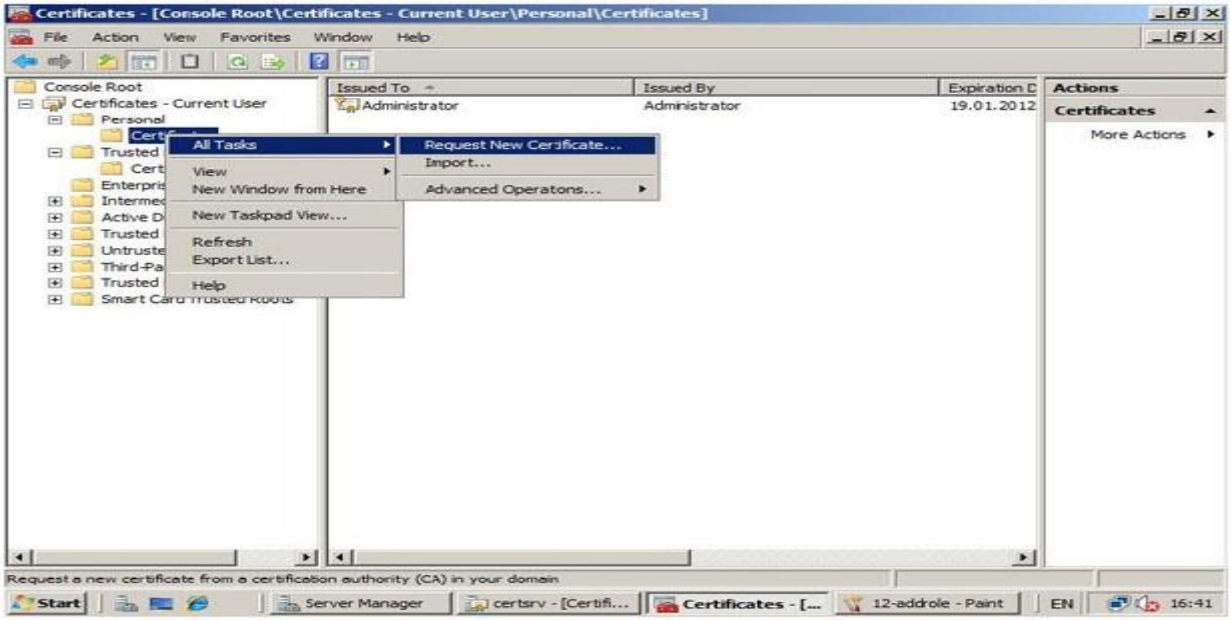


Рис. 16.Запрос сертификата

Вывод: В ходе работы мы ознакомились с вопросами использования цифровых сертификатов и рассмотрели возможности, которые предоставляет Windows Server 2008 по созданию собственно центра сертификации (Certification Authority – CA) на предприятии.

ЛАБОРАТОРНАЯ РАБОТА № 4
Шифрование данных при хранении – EFS

Шифрующая файловая система (EncryptingFileSystem–EFS) появилась в операционных системах семейства Windows, начиная с Windows 2000. Она позволяет шифровать отдельные папки и файлы на томах с файловой системой NTFS. Рассмотрим этот механизм подробнее.

Задание: рассмотреть шифрующая файловая система (EncryptingFileSystem–EFS).

Ход работы:

Пусть, у нас имеется сервер Windows Server 2008, входящий в домен, и три учетные записи, обладающие административными правами на сервере (одна из них - встроенная административная запись Administrator).

Пользователь User1 хочет защитить конфиденциальные файлы. Тут надо отметить, что хотя шифровать с помощью EFS можно и отдельные файлы, рекомендуется применять шифрование целиком к папке.

User1 с помощью оснастки Certificates запрашивает сертификат (можно выбрать шаблон User или BasicEFS). Теперь у него появляется ключевая пара и сертификат открытого ключа, и можно приступать к шифрованию.

Чтобы зашифровать папку, в ее свойствах на вкладке General нажимаем кнопку Advanced и получаем доступ к атрибуту, указывающему на шифрование файла.

Рис. 17. В свойствах папки устанавливаем шифрование

Работа EFS организована так, что одновременно сжатие и шифрование файлов и папок осуществляться не может. Поэтомунельзяразомустановитьатрибуты Compress contents to save disk и Encrypt contents to secure data (рис. 17).

При настройках по умолчанию, зашифрованная папка выделяется в проводнике зеленым цветом. Для зашифровавшего файл пользователя порядок работы с ним не изменится.

Теперь выполним "переключение пользователей" и зайдем в систему под другой учетной записью, обладающей административными правами, но не являющейся встроенной административной записью. Пусть это будет User2.

Несмотря на то, что User2 имеет такие же разрешения на доступ к файлу, что и User1, прочитать он его не сможет (рис. 18).

Также он не сможет его скопировать, т.к. для этого надо расшифровать файл. Но надо учитывать, что User2 может удалить или переименовать файл или папку.

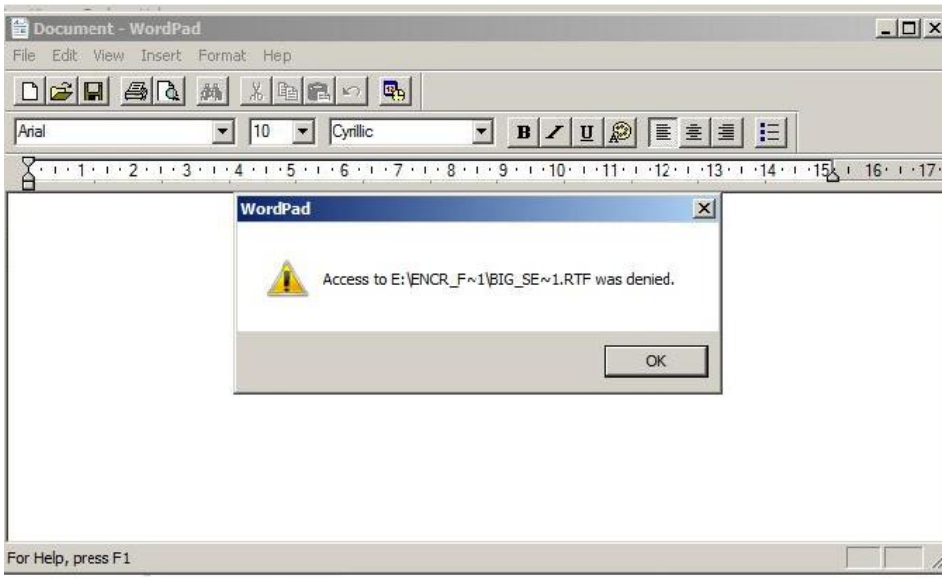


Рис. 18. Другой пользователь прочитать файл не сможет

Работая под первой учетной записью, запросим сертификат (если он не был получен ранее), после чего зашифруем папку с тестовым файлом, который не жалко потерять. Убедимся, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT.

Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.

Снова зайдем под первой учетной записью. В оснастке Certificates, удалим сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершим сессию пользователя в системе и войдите заново. Попробуем открыть зашифрованный файл.

Как мы убедились, если сертификат и соответствующая ему ключевая пара удалены, пользователь не сможет прочитать зашифрованные им же данные. В частности поэтому, в EFS введена роль агента восстановления. Он может расшифровать зашифрованные другими пользователями данные.

Реализуется это примерно следующим образом. Файл шифруется с помощью симметричного криптоалгоритма на сгенерированном системой случайном ключе (назовем его K1). Ключ K1 шифруется на открытом ключе пользователя, взятом из сертификата, и хранится вместе с зашифрованным файлом. Также хранится K1, зашифрованный на открытом ключе агента восстановления. Теперь либо пользователь, осуществлявший шифрование, либо агент восстановления могут файл расшифровать.

При настройке по умолчанию роль агента восстановления играет встроенная учетная запись администратора (локального, если компьютер не в домене, или доменная).

Выполнение работы:

Зайдем в систему под встроенной учетной записью администратора и расшифруем папку.

То, какой пользователь является агентом восстановления, задается с помощью групповых политик. Запустим оснастку Group Policy Management. В политике домена найдем группу Public Key Policies и там Encrypting File System, где указан сертификат агента восстановления (рис. 19). Редактируя политику (пункт Edit в контекстном меню, далее Policies —> Windows Settings —> Security Settings —> Public Key Policies —> Encrypting File System), можно отказаться от присутствия агентов восстановления в системе или наоборот, указать более одного агента (рис. 20).

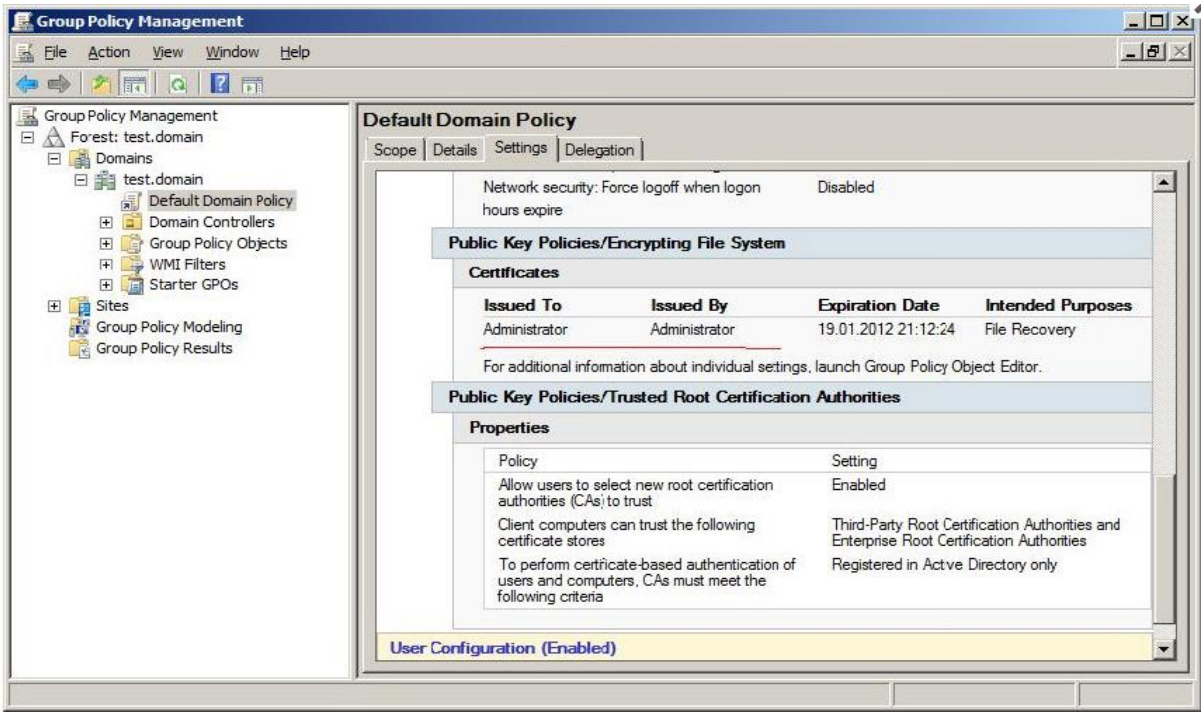


Рис. 19. Агент восстановления

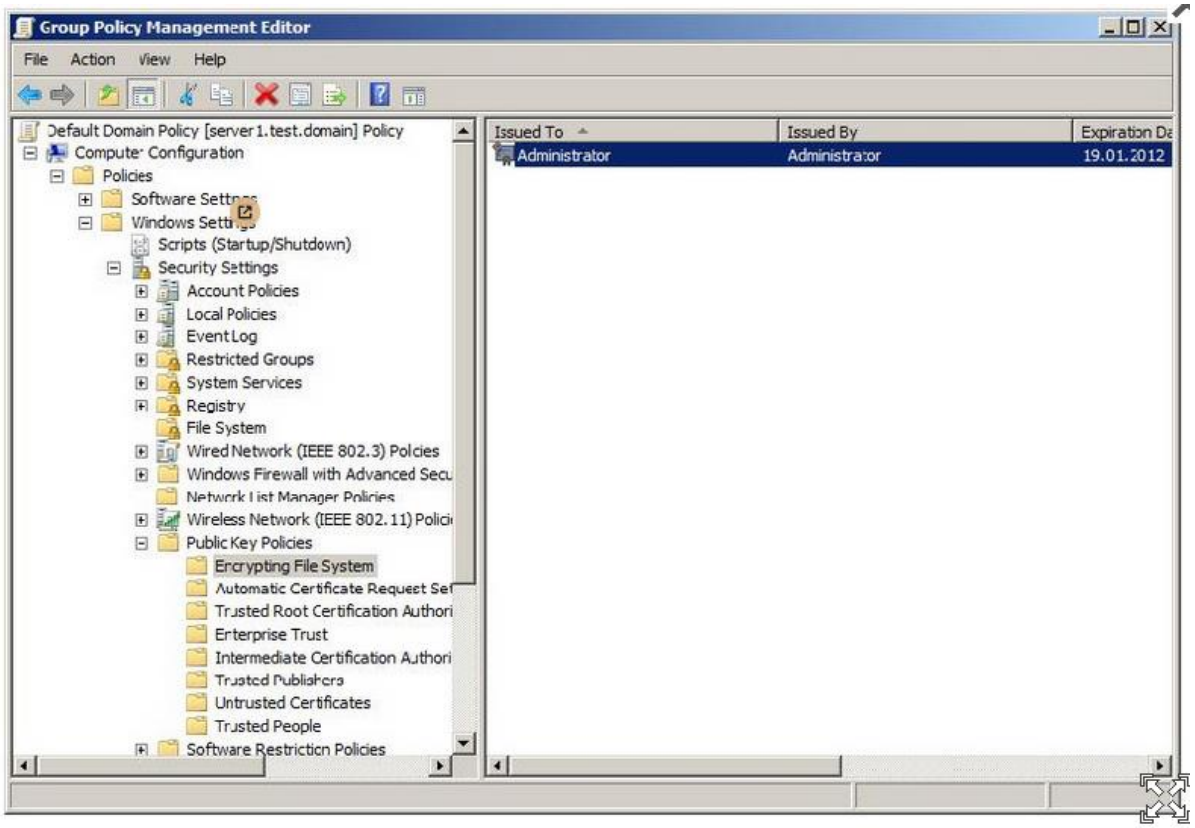


Рис. 20. Изменение агента восстановления

Отредактируем политику таким образом, чтобы убрать из системы агента восстановления (удалите в политике сертификат). Выполнив команду "gpupdate /force" (меню Start—>run—> gpupdate /force) примените политику.

Повторив действия из предыдущих заданий, убедимся, что теперь только тот пользователь, который зашифровал файл, может его расшифровать.

Теперь вернем в систему агента восстановления, но будем использовать новый сертификат. В редакторе политик находим политику Encrypting File System и в контекстном меню выбираем Create Data Recovery Agent. Это приведет к тому, что пользователь Administrator получит новый сертификат и с этого момента сможет восстанавливать шифруемые файлы.

Теперь рассмотрим, как можно предоставить доступ к зашифрованному файлу более чем одному пользователю. Такая настройка возможна, но делается она для каждого файла в отдельности.

В свойствах зашифрованного файла откроем окно с дополнительными параметрами, аналогичное представленному на рис. 17, для папки. Если нажать кнопку Details, будут выведены подробности относительно того, кто может получить доступ к файлу. На рис. 21 видно, что в данный момент это пользователь User1 и агент восстановления Administrator. Нажав кнопку Add можно указать сертификаты других пользователей, которым предоставляется доступ к файлу.

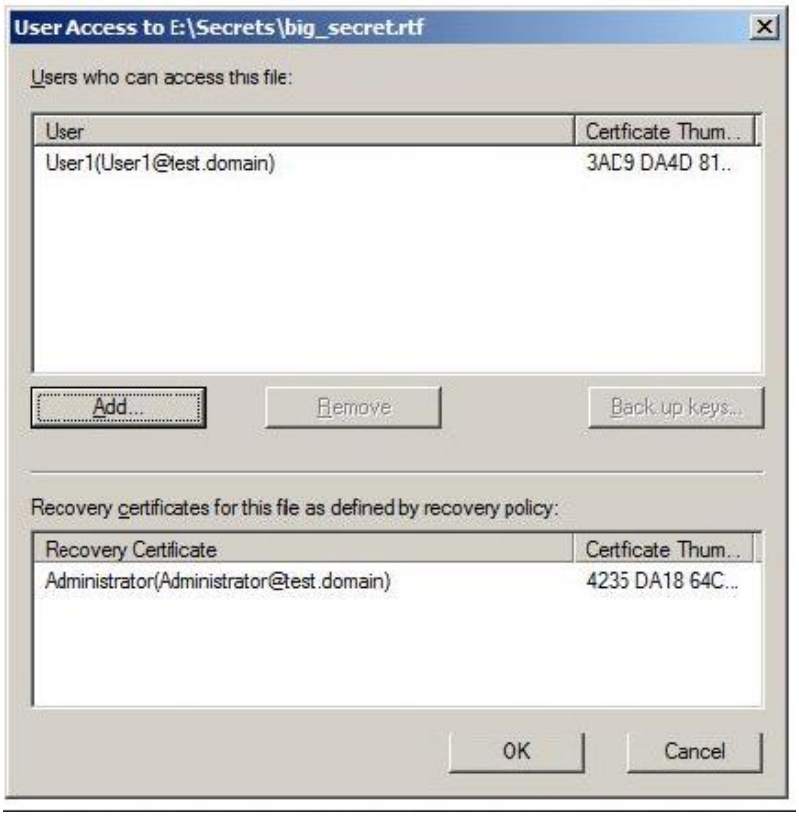


Рис. 21. Данные о пользователях, которые могут расшифровать файл

Вывод: в ходе проделанной лабораторной работы мы зашифровали файл с помощью шифрующей файловой системы (Encrypting File System – EFS). Мы убедились, что данная программа позволяет шифровать отдельные папки и файлы на томах с файловой системой NTFS.

ЛАБОРАТОРНАЯ РАБОТА № 5
УПРАВЛЕНИЕ РАЗРЕШЕНИЯМИ НА ФАЙЛЫ И ПАПКИ

Задание:

1. Освоить теоретические основы идентификаторов безопасности – SID.

2. Рассмотреть вопросы управления разрешениями на файлы и папки Windows.

3. Получить навыки управления доступом к файлам, которое позволяет избежать многих проблем, связанных с безопасностью, как на рабочей станции, так и на серверах (в особенности, выполняющих роль файлового сервера).

Ход решения:

Пользователи (как доменные, так и локальные), группы пользователей и компьютеры (далее будем называть их всех субъектами) имеют уникальные идентификаторы безопасности – SID. Под этим идентификатором система и "знает" субъекта. SID имеет уникальное значение в пределах домена и формируется во время создания пользователя или группы, либо когда компьютер регистрируется в домене.

Когда пользователь при входе в систему вводит имя и пароль, ОС выполняет проверку правильности пароля и, если пароль правильный, создает маркер доступа для пользователя. Маркер включает в себя SID пользователя и все SID'ы групп, в которые данный пользователь входит.

Для объектов подлежащих защите (таких как файлы, папки, реестр Windows) создается дескриптор безопасности. С ним связывается список управления доступом (Access Control List – ACL), который содержит информацию о том, каким субъектам даны те или иные права на доступ к данному объекту. Чтобы определить, можно ли предоставить запрашиваемый субъектом тип доступа к объекту, ОС сравнивает SID в маркере доступа субъекта с SID, содержащимися в ACL.

Разрешения суммируются, при этом запрещения являются более приоритетными, чем разрешения. Например, если у пользователя есть разрешение на чтение файла, а у группы, в которую он входит - на запись, то в результате пользователь сможет и читать, и записывать. Если у пользователя есть разрешение на чтение, а группе, в которую он входит, чтение запрещено, то пользователь не сможет прочитать файл.

Если говорить о файлах и папках, то механизмы защиты на уровне файловой системы поддерживаются только на дисках с файловой системой NTFS. Файловая система FAT (и ее разновидность – FAT32) не предполагает возможности хранения ACL, связанного с файлом.

Теперь перейдем к практической части работы. Выполняться она будет на компьютере с операционной системой Windows Server 2008, входящем в домен. Для выполнения работы понадобятся две учетные записи – администратора (далее будем называть его Administrator) и пользователя, не входящего в группу администраторов (будем называть его TestUser). Также понадобится тестовая группа (TestGroup). Все группы и учетные записи доменные, поэтому управление ими будем производить с помощью оснастки Active Directory Users and Computers.

Начнем с того, что работая под учетной записью Administrator, создадимновуюпапкуTest. В ее свойствах выберем вкладку Security (рис. 22). В отличие от предыдущих версий операционных систем Windows, в Windows Vista и Windows Server 2008 на этой вкладке можно только просматривать имеющиеся разрешения. Чтобы их изменять, надо нажать кнопку Edit, что даст возможность изменять список контроля доступа к файлу (рис.23).

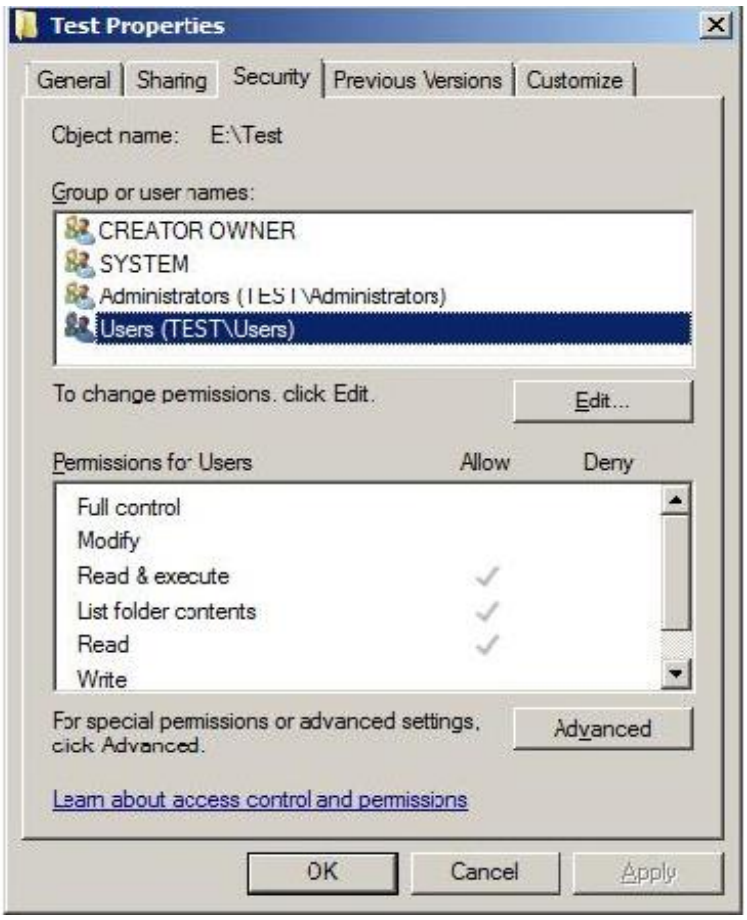


Рис. 22. Просмотр разрешений

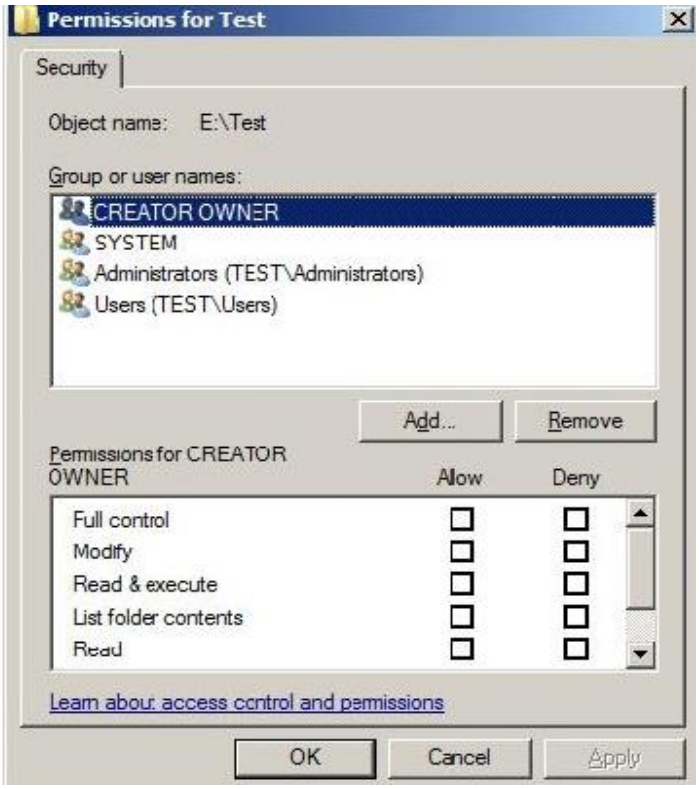


Рис.23. Изменение разрешений

Ход работы:

Выполним действия, аналогичные описанным выше. Убедимся, что пользователь TestUser отсутствует в списке доступа к папке, но есть в группе Users (последнее проверяется с помощью оснастки Active Directory Users and Computers, т.к. пользователь и группа доменные).

Выполним переключение пользователей, зайдем в систему под учетной записью TestUser, попробуем открыть папку и создать в ней новый файл.

Снова выполним переключение пользователей. Под учетной записью Administrator добавим в список доступа к файлу пользователя TestUser и дадим ему разрешение на изменение (modify). Пробуем снова выполнить задание.

Как мы убедились, можно добавлять пользователей в список доступа. Теперь попробуем под учетной записью Administrator удалить группу Users. Сделать это не удастся и появится предупреждение (рис. 24) о том, что эти разрешения наследуются от родительского объекта. Для того, чтобы отменить наследование надо на вкладке Security (рис. 24) нажать кнопку Advanced. Впоявившемсяокне(рис. 25)видно, чтоотмеченосвойство Include inheritable permissions from this object's parent. Это значит, что объект наследует родительский ACL, а в его собственный можно только добавлять разрешения или запрещения. Если нажать кнопку Edit и сбросить эту галочку будет задан вопрос, что делать с унаследованным списком – его можно скопировать (Copy) в ACL объекта или убрать (Remove). Чаще всего, чтобы не потерять нужные настройки, выполняется копирование, а потом уже список исправляется.

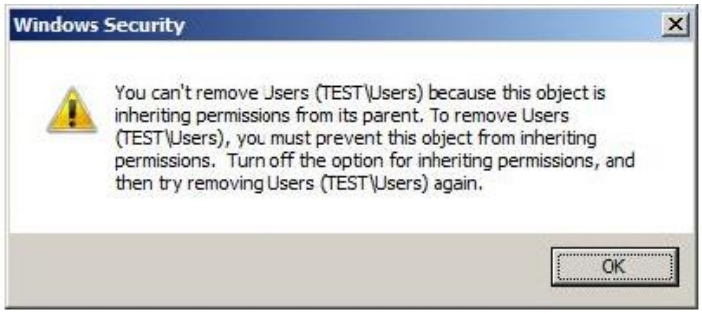


Рис. 24. Предупреждение

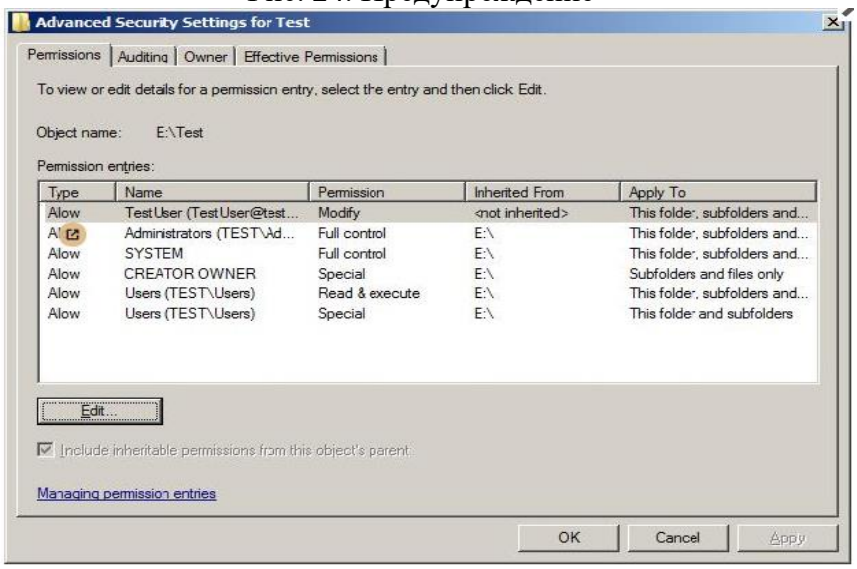


Рис. 25. Дополнительные параметры безопасности

Удалим группу Users из ACL для папки. Если редактировать разрешения пользователя из окна дополнительных параметров безопасности, то увидим список разрешений, отличный от того, что был ранее (рис. 26).

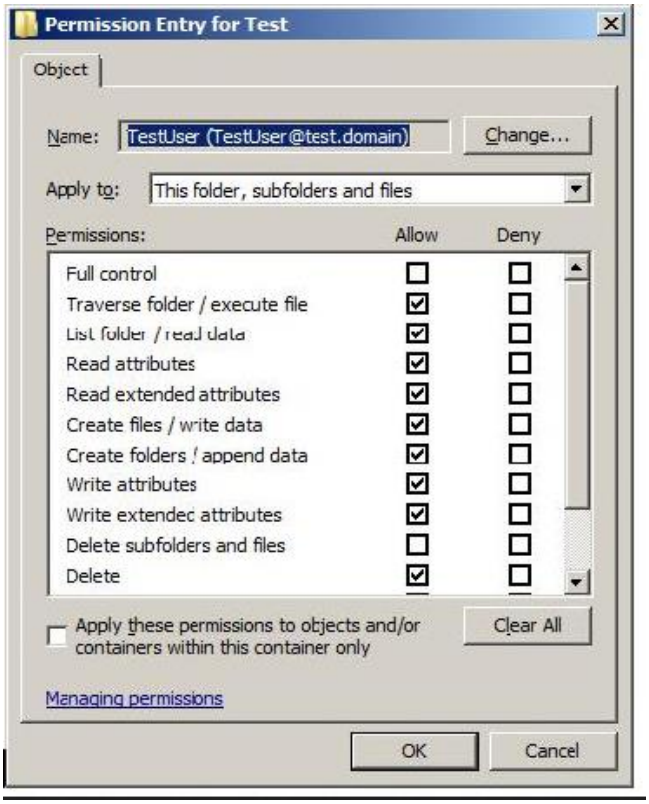


Рис. 26. Специальные разрешения

Это так называемые специальные разрешения. Виденные ранее стандартные разрешения (чтение/read, запись/write и т.д.) состоят из специальных. Соответствие между ними описано на рис. 27 (набор разрешений для папок и файлов несколько отличается, но понять какие к чему относятся можно по названиям). Более подробно с этой темой можно ознакомиться, например, по справочной системе Windows.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Рис. 27. Соответствие между специальными и стандартными разрешениями

Как уже ранее отмечалось, при определении разрешения на доступ, учитываются разрешения и запрещения, как для самого пользователя, так и для всех групп, в которые он входит. Для того, чтобы узнать действующее (эффективное) разрешение, можно воспользоваться вкладкой Effective Permissions (рис. 25). Там, нажав кнопку Select, можно выбрать пользователя или группу, для которой будет показано эффективное разрешение.

Проверим, чтобы у пользователя TestUser на папку, с которой работаем, было разрешение modify. Проверим действующее эффективное разрешение.

Не заканчивая сеанса пользователя, переключитесь в сеанс пользователя Administrator. Добавьте в список разрешений на папку запрещение для группы TestGroup всех видов доступа (выберите Deny для разрешения Full Control). Внесите пользователя TestUser в группу TestGroup. Посмотрите эффективное разрешение для пользователя TestUser.

Переключимся в сеанс пользователя TestUser. Попробуем открыть папку и создать документ. Завершим сеанс TestUser (выполните выход из системы) и снова войдем в систему. Повторно попробуем открыть папку и создать документ.

Теперь рассмотрим вопросы, связанные с владением папкой или файлом. Пользователь, создавший папку или файл, становится ее владельцем. Текущего владельца объекта можно узнать, если в окне дополнительных параметров безопасности (рис.4) выбрать вкладку Owner.

Владелец файла может изменять разрешения на доступ к этому файлу, даже в том случае, если ему самому доступ запрещен.

Порядок смены владельца файла в Windows Server 2008 отличается от того, что было в предыдущих версиях ОС. Ранее, администратор или пользователь, имеющий на файл (папку) право Take Ownership могли стать владельцами файла. Причем, владельцем мог быть или конкретный пользователь, или группа Администраторы (Adminisrators) – другую группу владельцем было не назначить.

В Windows Server 2008 администратор (или член группы администраторов) может не только сам стать владельцем, но и передать право владения произвольному пользователю или группе. Но эта операция рассматривается как привилегированная, и доступна не всякому пользователю, имеющему право на файл.

На рис. 28 показано, что Администратор сделал владельцем папки Test группу TestGroup.

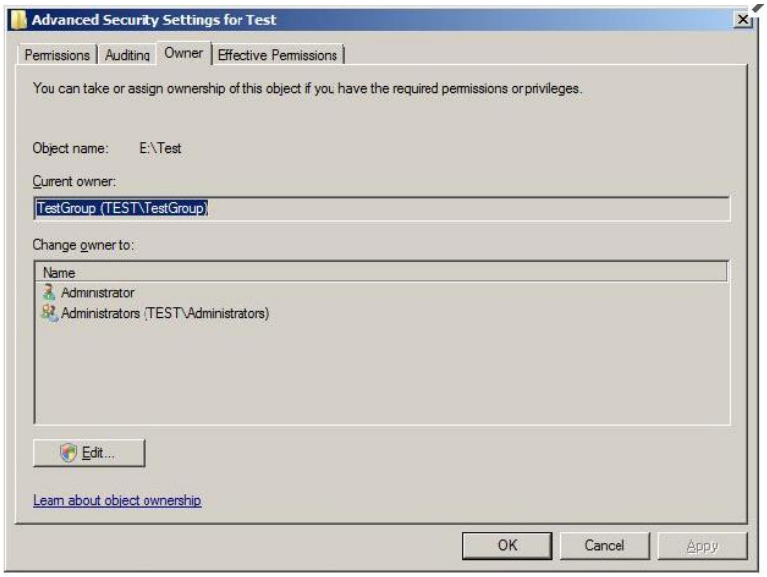


Рис. 28. Смена владельца объекта

Выполним передачу права владения группе TestGroup, куда входит пользователь TestUser. Зайдя под этой учетной записью, измените разрешения так, чтобы TestUser смог работать с папкой.

При использовании компьютера с Windows Server 2008 в качестве файлового сервера, важно учитывать, что на предоставляемые в общий доступ папки, отдельно устанавливаются разрешения, регулирующие доступ к ним по сети. Сделать это можно в свойствах папки на вкладке Sharing (рис. 29). В этом случае, при доступе по сети действуют и разрешения на общую папку, и разрешения NTFS. В результате получаем наиболее строгие ограничения. Например, если на общую папку установлено "только чтение", а в разрешениях NTFS - "изменение", то в итоге, подключающийся по сети пользователь сможет только читать файлы. А тот же пользователь при локальном доступе получает право на изменение (разрешения на общую папку влиять не будут).

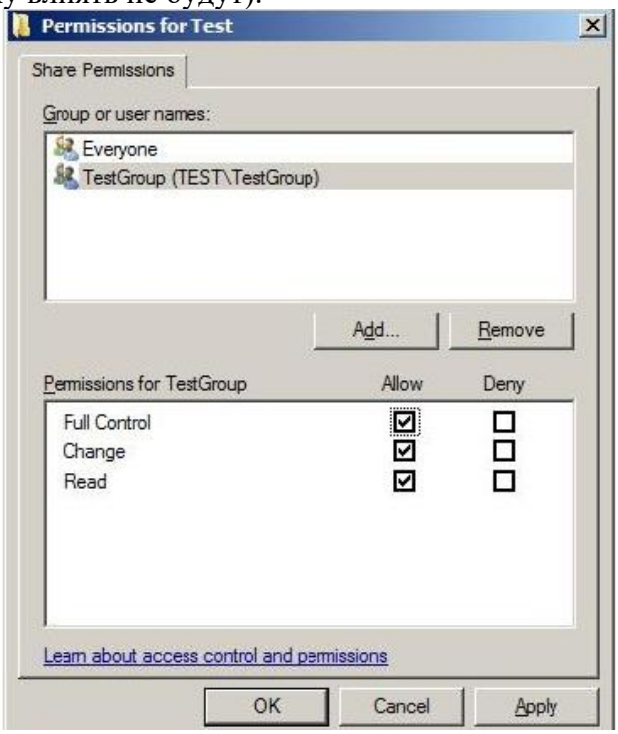


Рис. 29. Разрешения на общую папку

Вывод: данную лабораторную работу мы посвятили вопросам управления разрешениями на файлы и папки Windows. Мы работали под учетной записью Administrator.

ЛАБОРАТОРНАЯ РАБОТА № 6
РЕЗЕРВНОЕ КОПИРОВАНИЕ В WINDOWS SERVER 2008

Задание: познакомиться со средствами организации резервного копирования в операционной системе Microsoft Windows Server 2008.

Ход решения:

С точки зрения управления рисками, важность процедуры резервного копирования очень высока. В тех случаях, когда реализация угрозы приводит к изменению или удалению данных, повреждению программных компонент системы, резервное копирование позволяет снизить причиненный ущерб и значительно ускорить восстановление системы.

При разработке политики резервного копирования нужно определить, как минимум, следующие параметры:

- частоту выполнения резервных копий;
- порядок восстановления данных из резервных копий;
- объем носителей информации, выделяемых для хранения резервных копий;
- количество хранимых копий;
- вопросы обеспечения безопасности носителей резервных копий.

Утилиты резервного копирования Windows Server 2008 существенно отличаются от того, что было в Windows Server 2003 (где эти задачи решались с помощью утилиты ntbackup). Чтобы их использовать, для начала требуется их установить (по умолчанию, они не устанавливаются). Делается это с помощью оснастки Server Manager, где надо выбрать пункт Add Feature в разделе Features (рис. 30) и в появившемся списке выбрать пункт Windows Server Backup Features (рис. 31).

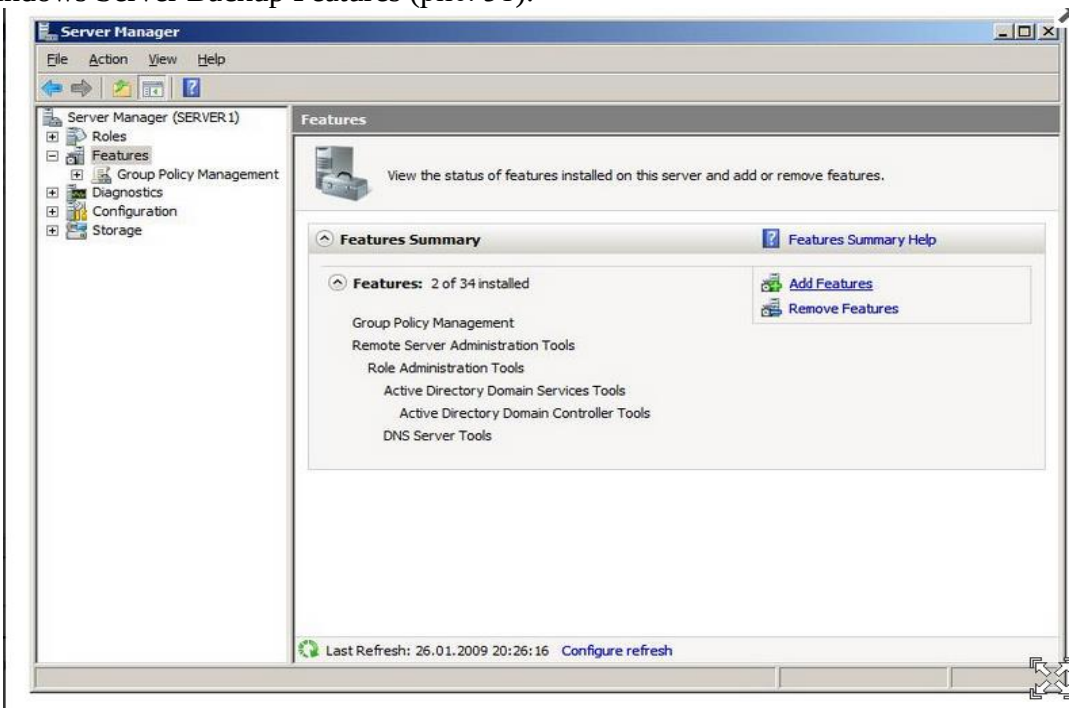


Рис. 30. Оснастка Server Manager позволяет добавить компоненты

Как видно на рис. 31, предлагается выбрать следующие опции:

- Windows Server Backup;
- Command-line tools (утилиты командной строки).

Установка последних, позволяет управлять резервным копированием с помощью сценариев и требует установки Windows PowerShell. Но для выполнения лабораторной будет достаточно установить только Windows ServerBackup.

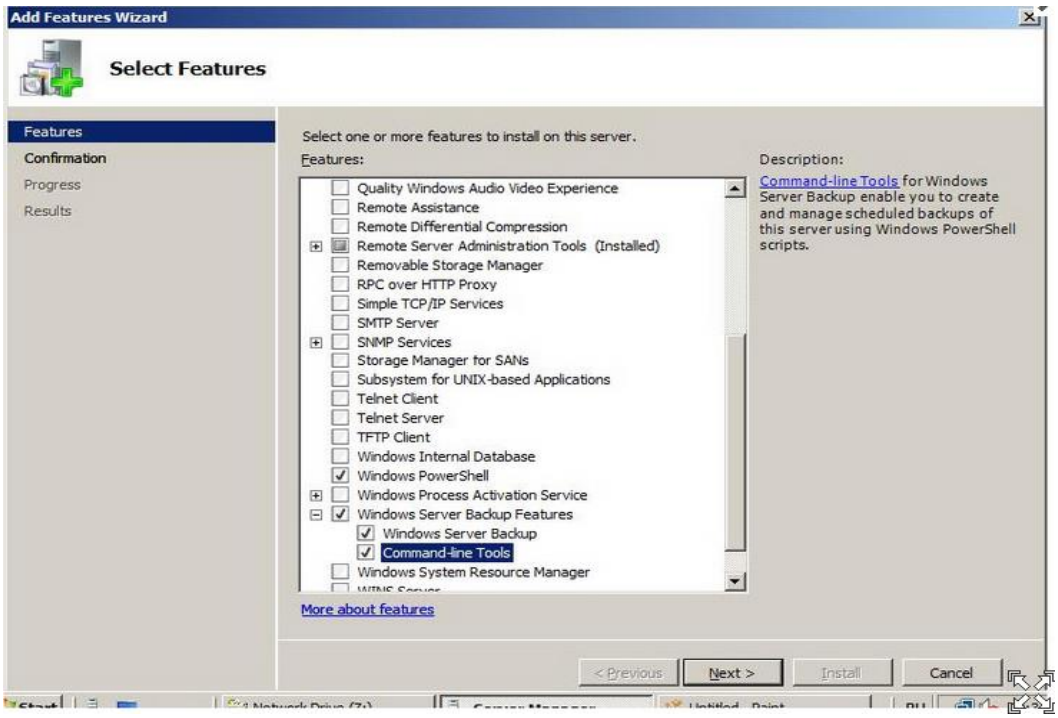


Рис. 31. Добавляем утилиты администрирования

После установки, в меню Administrative Tools становитсядоступнойоснастка Windows Server Backup. С ее помощью можно проводить резервное копирование данных на локальном или удаленном компьютере (если это разрешено настройками).

Рассмотрим, как это происходит. Запустим утилиту. Резервное копирование может проводить пользователь, состоящий в группе Administrators (Администраторы) или Backup Operators (Операторы архива). При этом, у членов группы Backup Operators при запуске оснастки Windows Server Backup будет дополнительно запрашиваться пароль (в окне User Account Control), т.к. эти операции относятся к разряду потенциально опасных.

В окне оснастки в списке доступных действий (Actions), расположенном в правой части экрана, выберем опцию Backup Once … (т.е. однократная архивация). Запустившийся мастер резервного копирования предложит выбор между настройками для уже запланированного копирования (The same options that you used in the Backup Schedule Wizard for scheduled backups) и новыми (Different options). Нужно выбрать второй вариант (если, как в нашем примере, утилита ранее не использовалась, то первый пункт списка будет неактивен).

Следующее окно мастера позволяет выбрать, производить ли полное резервное копирование или копирование отдельных разделов (рис. 32). Здесь проявляется первое отличие новых инструментов – резервное копирование отдельных папок и файлов производить нельзя, только логический диск целиком.

Хотелось бы также обратить внимание на надпись в нижней части экрана, там дается ссылка на раздел справки, описывающий выполнение с помощью утилиты командной строки резервного копирования только состояния системы (System State).

Выберем вариант Custom.

Тогда на следующем экране появится список дисков (рис. 33). Устанавливая или снимая отметки, можно указать, данные с каких дисков помещаются в резервную копию. Опция Enable System Recovery включает в архив разделы, где находятся компоненты операционной системы и файлы необходимые для загрузки (т.е. отметку напротив этих разделов будет не снять).

Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис. 33, и

переходим к следующей стадии, на которой нужно определить, куда будет производиться копирование. Это может быть локальный диск (жесткий диск, пишущий DVD-привод и т.д.) или сетевая папка. Надо учитывать, что архивная копия не может сохраняться на диск, входящий в перечень архивируемых. Также нельзя сохранить архив на диск, где хранятся файлы операционной системы.

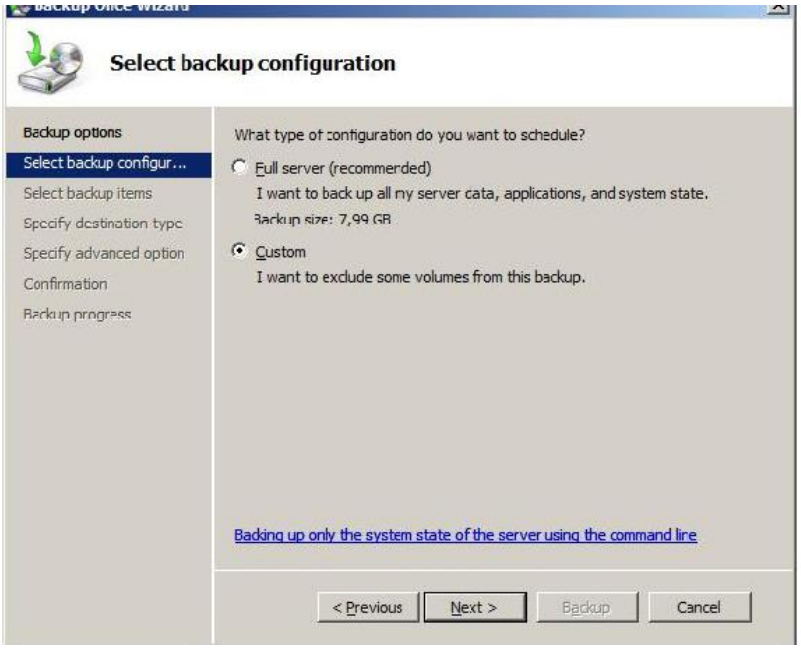


Рис. 32. Выбор между полным резервным копированием и копированием отдельных дисков

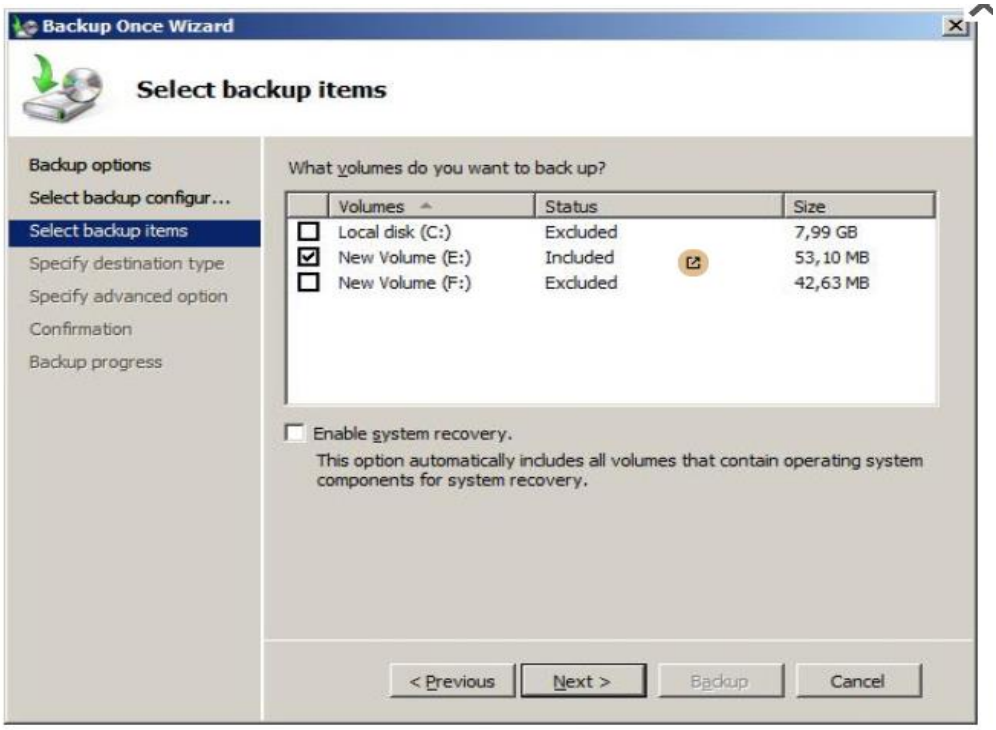


Рис. 33. Выбор дисков для резервного копирования

Учитывая все вышеизложенное, в рассматриваемом примере можно сделать резервную копию диска E: на диск F:, в сетевую папку или на DVD-диск. Выберем первый

вариант, что и укажем в следующем окне мастера. После чего будет предложено выбрать тип резервного копирования (рис. 34).

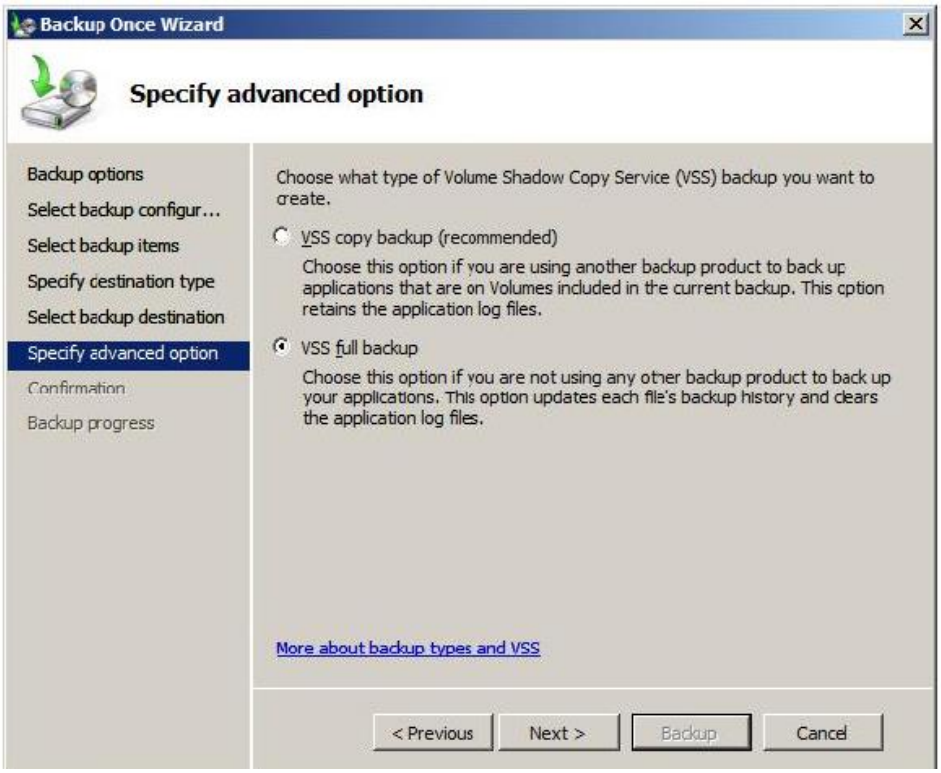


Рис. 34. Выбор типа копирования

Служба Volume Shadow Copy Service (VSS) может при резервном копировании отмечать файлы, как помещенные в архив, или не делать это. Если кроме средств Windows Server 2008 используются и другие продукты для резервного копирования, рекомендуется выбрать вариант VSS copy backup. Если такого нет, можно смело выбирать вариант VSS full backup.

В следующем окне мастера будет запрошено подтверждение и, если оно получено, запустится резервное копирование.

В результате, в нашем примере на диске F: появится каталог WindowsImageBackup, в нем будет создан подкаталог, названный по имени архивируемого сервера, куда и попадет копия.

На учебном сервере выберем раздел для резервного копирования.

С учетом рассмотренных ограничений и объема копируемого раздела, выберем место для размещения копии. Определим, от имени какой учетной записи будет проводиться эта операция.

Выполним однократное резервное копирование выбранного раздела.

Теперь рассмотрим порядок восстановления данных из резервной копии.

В первой части лабораторной работы была сделана резервная копия раздела E:. Пусть понадобилось восстановить содержимое одной из папок из этого раздела. При этом требуется сравнить текущее содержимое папки с архивной копией, т.е. восстанавливать нужно в другую папку.

Запускаем оснастку Windows Server Backup и в списке Actions выбираем Recover (восстановление). Мастер восстановления уточняет, какой сервер будет восстанавливаться, после чего представит перечень имеющихся резервных копий (рис. 35).

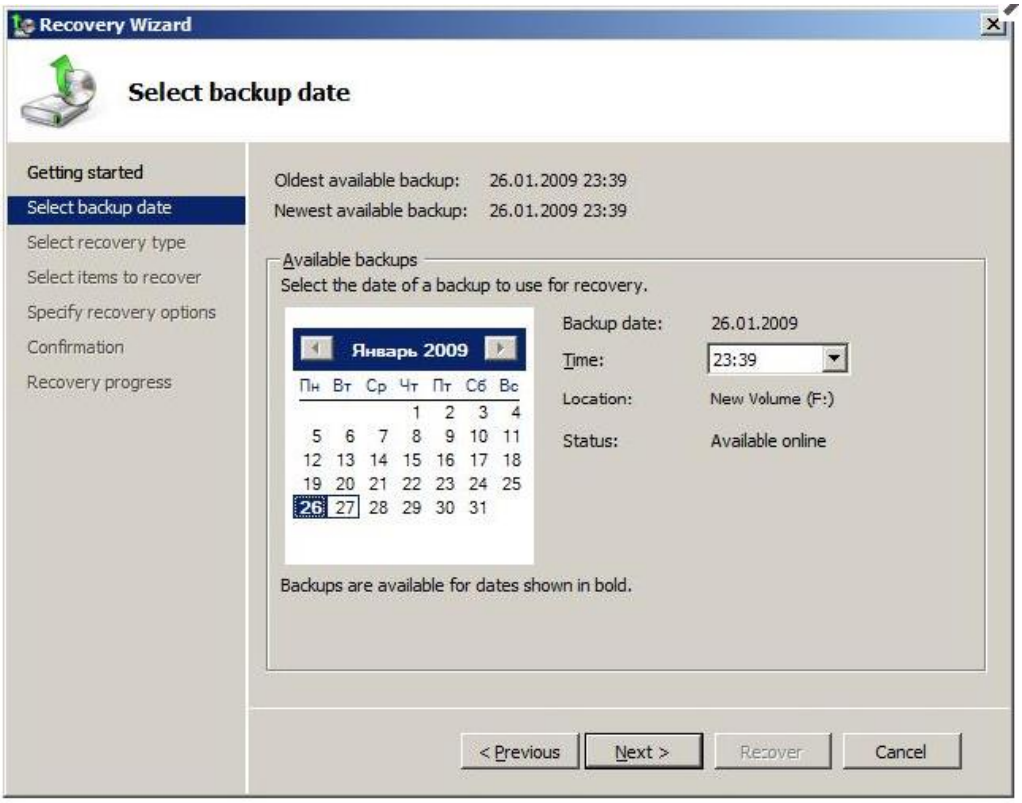


Рис. 35. Перечень доступных резервных копий для выбранного сервера

В следующем окне запрашивается, что именно восстанавливается. Нас интересует отдельная папка, потому выбираем вариант Files and folders (рис. 36). Другие варианты - восстановление зарегистрированных приложений и восстановление раздела диска целиком.

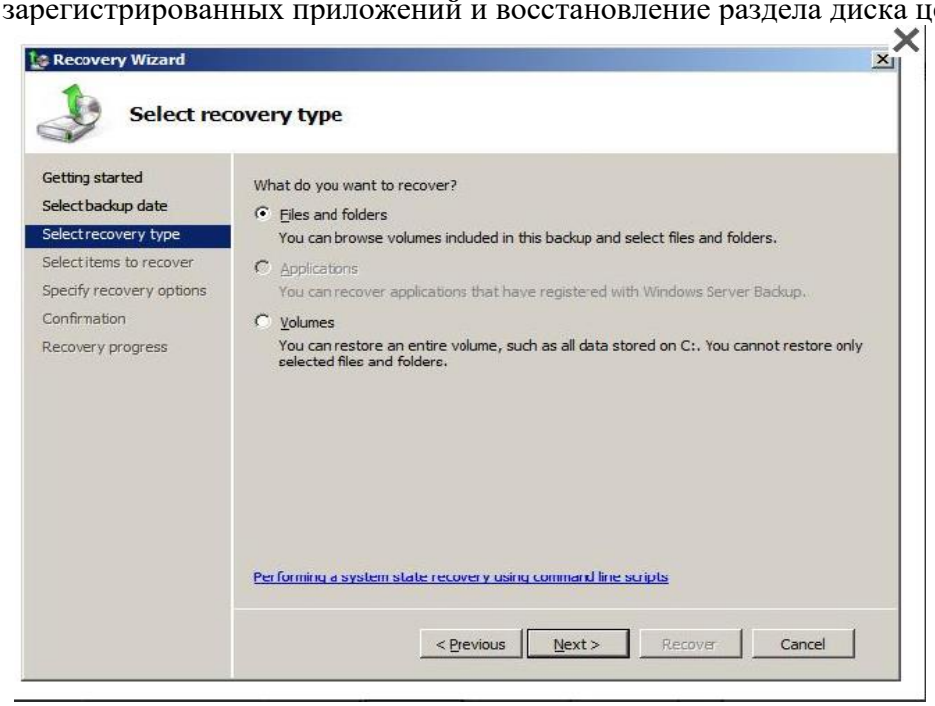


Рис. 36. Выбор типа восстановления

В следующем окне мастера в выпадающем списке нужно найти и выделить выбранную для восстановления папку. Если восстановить нужно несколько объектов, их

выделяют совместно, удерживая клавишу Ctrl (или Shift для выделения диапазона). После этого выбирается путь для восстановления и задаются параметры. В нашем примере, мы хотим восстановить выбранную папку с файлами во вновь созданную папку restored (рис.37).

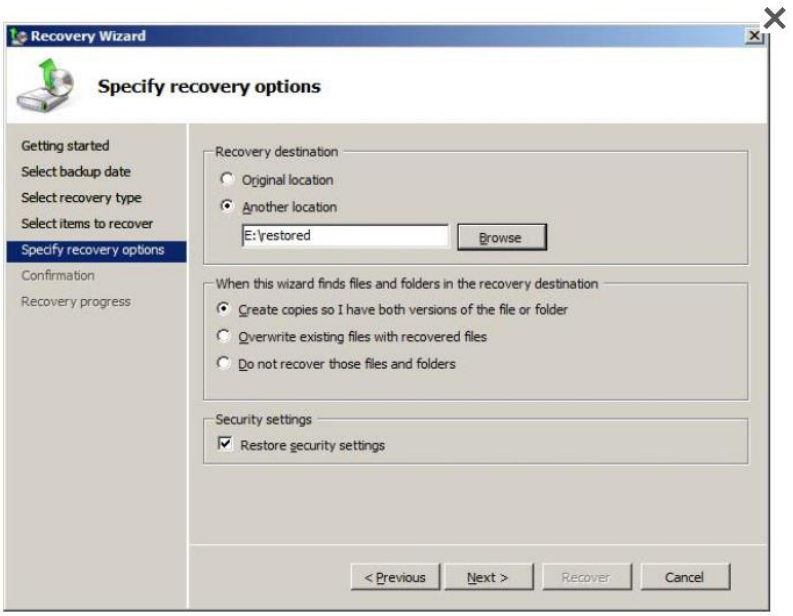


Рис. 37. Параметры восстановления

Кроме пути (исходный или альтернативный), выбирается вариант действий при совпадении имен файлов и папок. Это особенно актуально, если восстанавливать файлы в исходную папку. Вариантов три – создавать копии, перезаписывать имеющиеся объекты восстанавливаемыми, оставить имеющиеся объекты.

Последний из выбираемых в этом окне параметров указывает на то, восстанавливать ли настройки безопасности (т.е. списки доступа к файлам). После выбора всех параметров будет запрошено подтверждение и начнется восстановление.

Выберем из архива, созданного в предыдущей части работы, группу файлов для восстановления. Восстановите их в первый раз по исходному пути с сохранением копий, во второй раз - по альтернативному пути. Опишите, в чем разница в полученных результатах.

Теперь рассмотрим организацию резервного копирования по расписанию. Дляэтогов Windows Server Backup выберемопцию Backup Schedule. Первое окно запустившегося мастера информирует, что прежде чем устанавливать резервное копирование по расписанию, нужно определить:

– что будет копироваться (полное резервное копирование сервера или отдельные диски);

– как часто надо проводить копирование;

– где размещать копии.

Пусть требуется ежедневно делать резервное копирование диска раздела с операционной системой. В окне мастера аналогичном рис. 32, выбираем вариант Custom, в окне аналогичном рис. 33 – диск C (на котором расположена операционная система). Указываем расписание (рис. 38).

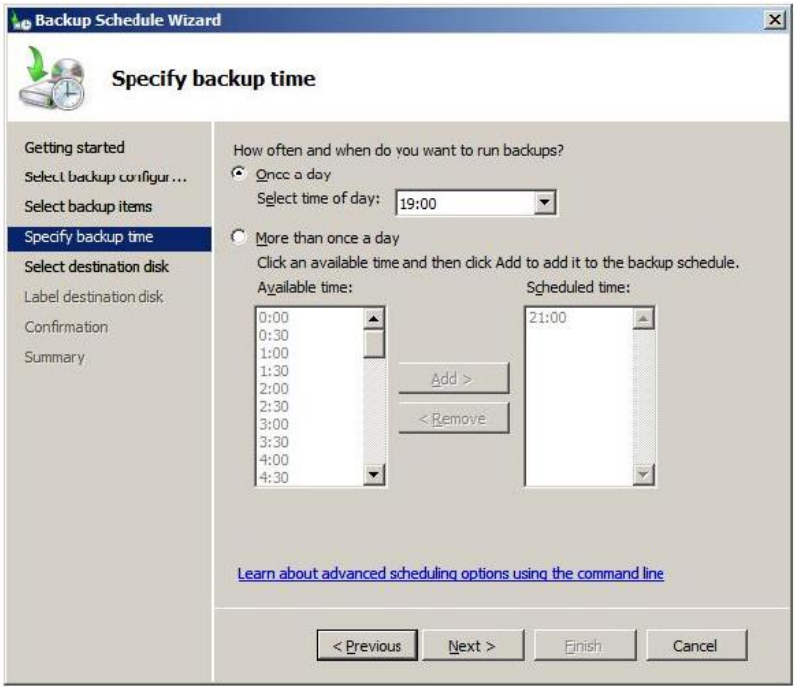


Рис. 38. Расписание резервного копирования

Дальше определяется диск (рис. 39), он может быть не отформатирован. Диску будет назначена метка с названием сервера и датой определения резервного копирования, после чего будет проведено форматирование. Диску не назначается буква и он не будет доступен пользователям как обычный диск.

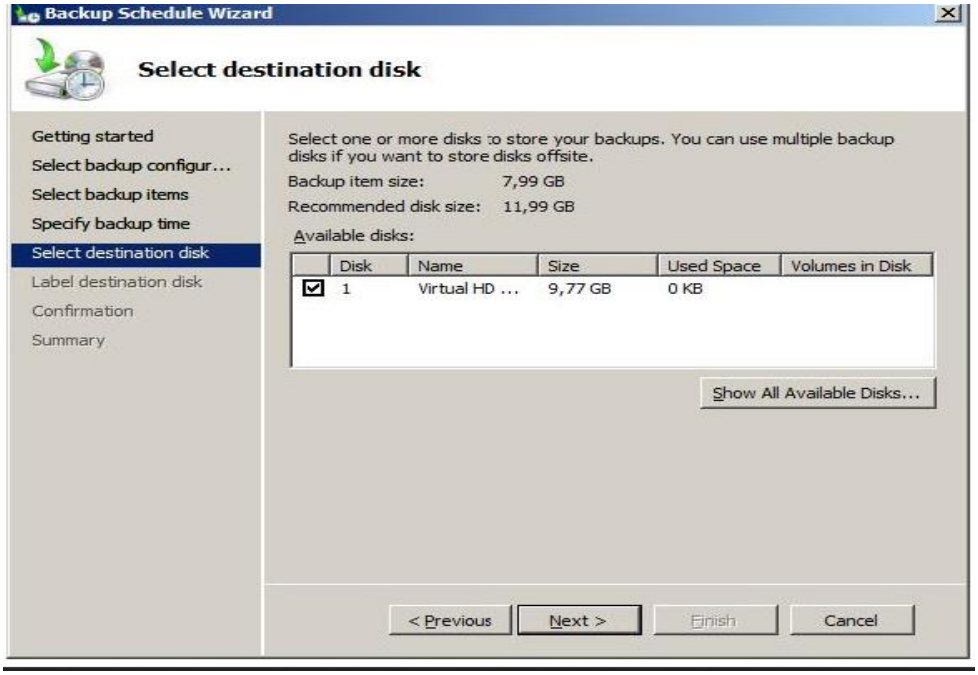


Рис. 39. Диск для хранения резервных копий

Когда работа по настройке автоматической архивации завершена, можно сделать дополнительные настройки, повышающие быстродействие для отдельных дисков. Дляэтоговсписке Actions воснастке Windows Server Backup выберитепункт Configure

Performance Settings. В открывшемся окне (рис. 40) можно установить, какой тип резервного копирования производить для диска – полное (full) или добавочное (Incremental). По умолчанию используется полное. Добавочное помещает в архив только измененные с момента последнего архивирования файлы, это позволяет провести резервное копирование быстрее, но более существенно снижает производительность сервера в период копирования (т.к. надо проводить проверку).

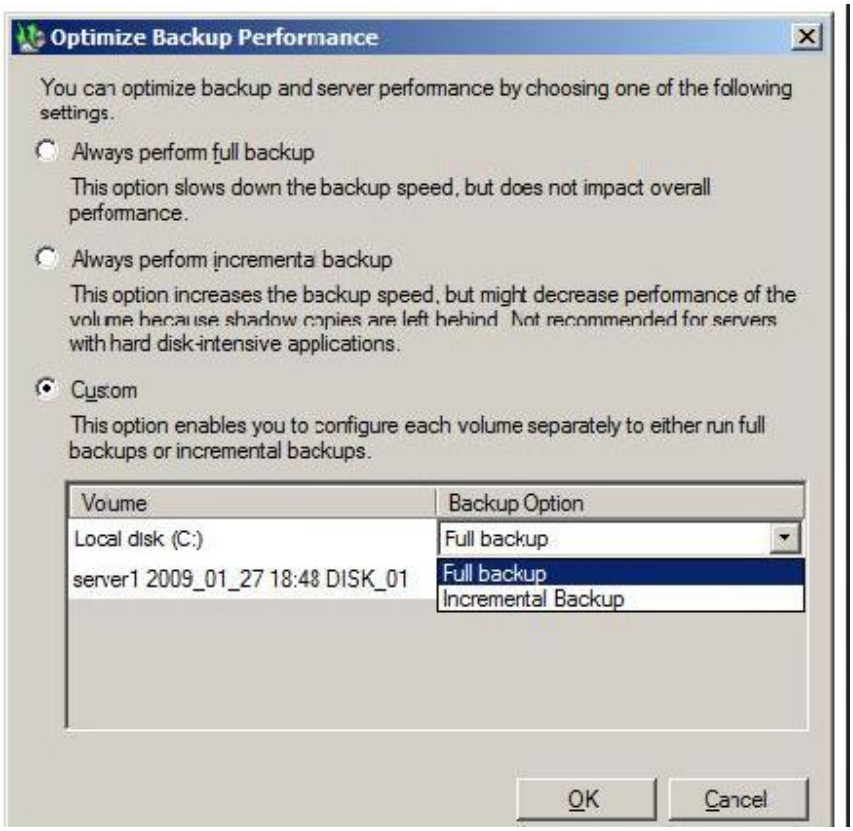


Рис. 40. Выбор типа резервного копирования для диска

Порядок восстановления такой же, как и при однократном копировании.

Кстати, посмотреть параметры запланированного резервного копирования можно с помощью оснастки Task Scheduler (рис. 41).

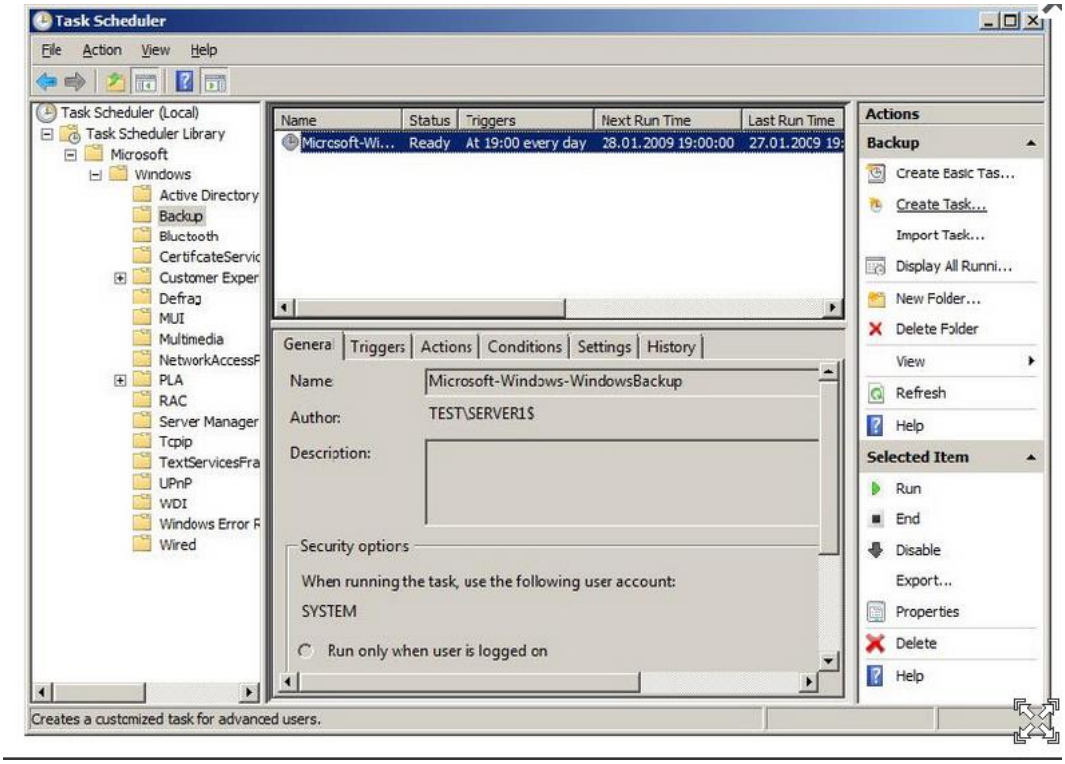


Рис. 41. Параметры созданного задания

Вывод: в ходе лабораторной работы мы познакомились со средствами организации резервного копирования в операционной системе Microsoft Windows Server 2008. При разработке политики резервного копирования мы определили следующие параметры:

– частоту выполнения резервных копий;
– порядок восстановления данных из резервных копий;
– объем носителей информации, выделяемых для хранения резервных копий;
– количество хранимых копий;
– вопросы обеспечения безопасности носителей резервных копий.

ЛАБОРАТОРНАЯ РАБОТА № 7
ПРИМЕНЕНИЕ РЕГРЕССИОННОГО АНАЛИЗА ПРИ ОЦЕНКЕ РИСКОВ

Задание:

В нижеприведенной таблице (табл. 2) приведена информация по месячным доходностям за 2017 г. индекса РТС и по пяти доходностям новых отраслей индексов российской торговой системы (РТС): нефть и газ (RTSog); электроэнергетика (RTSeu); телекоммуникации (RTStl); промышленность (RTSin); потребительские товары и розничная торговля (RTScr).

Таблица 2

Информация по месячным доходностям за 2017 г.

Месяц	Доходности индексов за месяц (%)					
		1	2	3	4	5
	RTS	RTStl	RTSog	RTSin	RTScr	RTSeu
Январь 2017	-5,055	4,406	-9,839	2,121	-1,511	9,360

Продолжение таблицы 2

Февраль 2017	4,456	-3,918	-3,285	5,737	4,212	7,660
Март 2017	1,555	7,600	3,853	1,915	9,241	9,332
Апрель 2017	-0,011	4,144	-2,913	2,08	2,595	-3,013
Май 2017	-8,018	-6,413	-9,633	3,039	-4,965	-4,490
Июнь 2017	6,593	1,843	4,751	7,145	4,553	6,897
Июль 2017	5,072	0,604	4,853	12,003	3,406	-0,714
Август 2017	-3,715	-1,157	-3,349	4,415	-2,282	-6,487
Сентябрь 2017	7,912	6,07	7,624	-0,059	0,700	2,514
Октябрь 2017	7,301	5,223	6,746	-0,251	5,521	3,915
Ноябрь 2017	-0,133	3,506	0,371	2,529	0,778	-0,580
Декабрь 2017	3,171	4,042	3,896	12,414	4,491	5,218

Требуется:

Определить характеристики каждой ценной бумаги: α, β, рыночный (систематический) риск, собственный (несистематический) риск, R2. Сформировать портфель минимального риска из двух видов отраслевых индексов RTStl и RTSog (при условии, что обеспечивается доходность портфеля (mp) не менее, чем по безрисковым ценным бумагам (облигациям), - 0,5% с учетом общего индекса рынка. Построить линию рынка капитала (CML). Построить линию рынка ценных бумаг (SML).

Ход решения:

Для построения модели Марковица на первом этапе необходимо представить исходные данные в Excel в виде следующей таблицы.

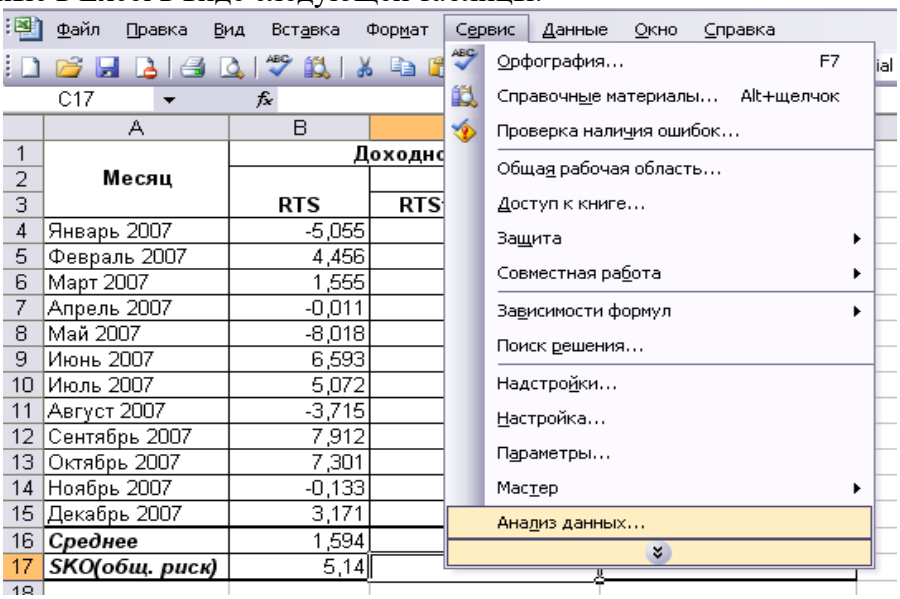


Рис.42. Ввод исходных данных.

Применение регрессионного анализа

Построим модель зависимости доходности индекса телекоммуникации (RTStl) от индекса рынка.

Параметры модели найдем с помощью инструмента Регрессия "Пакета анализа" Excel. Для проведения регрессионного анализа выполним следующие действия:

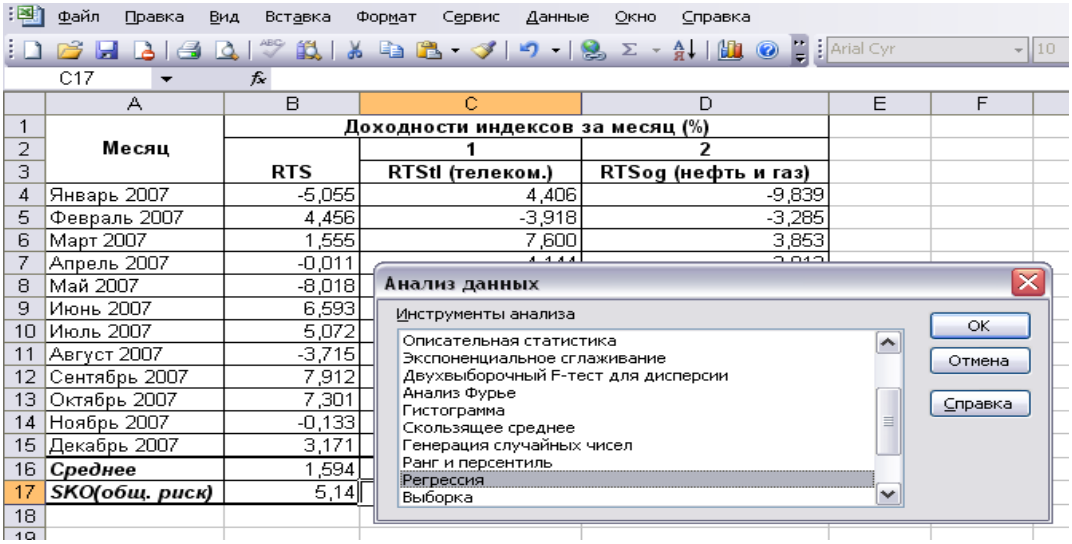
Выбираем команду "Данные" → "Анализ данных".

В диалоговом окне "Анализ данных" выбираем инструмент "Регрессия", а затем щелкаем по кнопке ОК.

В диалоговом окне "Регрессия" в поле "Входной интервал Y" вводим адрес одного диапазона ячеек, который представляет зависимую переменную. В поле "Входной интервал X" вводим адрес диапазона, который содержит значения независимых переменных.

Выбираем параметры вывода "новый рабочий лист".

В поле "Остатки" проставляем необходимые флажки.



	A	B	C	D	E	F
1	Месяц	Доходности индексов за месяц (%)				
2			1	2		
3		RTS	RTStl (телеком.)	RTSog (нефть и газ)		
4	Январь 2007	-5,055	4,406	-9,839		
5	Февраль 2007	4,456	-3,918	-3,285		
6	Март 2007	1,555	7,600	3,853		
7	Апрель 2007	-0,011				
8	Май 2007	-8,018				
9	Июнь 2007	6,593				
10	Июль 2007	5,072				
11	Август 2007	-3,715				
12	Сентябрь 2007	7,912				
13	Октябрь 2007	7,301				
14	Ноябрь 2007	-0,133				
15	Декабрь 2007	3,171				
16	*Среднее*	1,594				
17	*SKO(общ. риск)*	5,14				
18						

Рис.43.Запуск анализа данных.

Результаты регрессионного анализа

Результаты регрессионного анализа содержатся в таб.3-5. Рассмотрим содержание этих таблиц. Во втором столбце таб.2 содержаться оценки параметров уравнения регрессии α и β. В третьем столбце содержаться стандартные ошибки коэффициентов уравнения регрессии, а в четвертом - t-статистика, используемая для проверки значимости коэффициентов уравнения регрессии.

Таблица 3

Оценка параметров уравнения регрессии

	Коэффициенты	Стандартная ошибка	t-статистика
Y-пересечение	1,613	1, 206	1,337
Индекс РТС	0,345	0,233	1,477

Уравнение регрессии зависимости доходности отраслевого индекса RTStl (m1) от индекса РТС (mr) имеет вид:

m1=1,613+ 0,345* mr

Таблица 4

Регрессионная статистика

Множественный R	0,423
R-квадрат	0,179
Нормированный R-квадрат	0,097
Стандартная ошибка	3,976
Наблюдения	12

Таблица 5

Дисперсионный анализ

	df	SS	MS	F	Значимость F
Регрессия	1	34,494	34,494	2,182	0,170
Остаток	10	158,067	15,807		
Итого	11	192,561			

Собственный (несистематический) риск отраслевого индекса RTStl (m1) равен $\sigma 2\varepsilon 1=\sum \varepsilon 2/ (N-1) =158,067/11= 14,37$.

Аналогично построим модель зависимости доходности отраслевого индекса RTSog (m2) от индекса РТС (mr), для этого выполним все вышеуказанные действия.

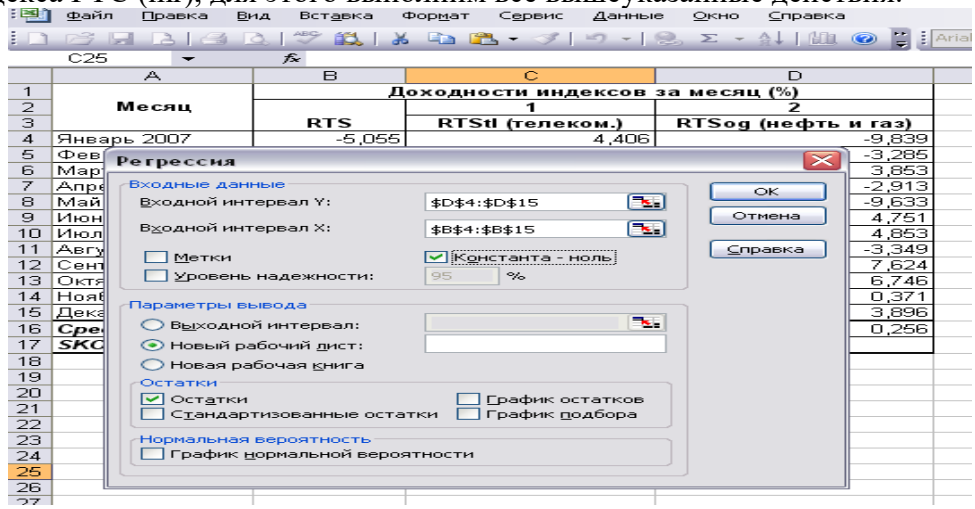


Рис.44. Заданы интервалы входных данных.

В результате построения второй модели получаем следующие результаты:

Таблица 6

Результаты построения второй модели

	Коэффициенты	Стандартная ошибка	t-статистика
Y-пересечение	-1,410	0,868	-1,624
Индекс РТС	1,045	0,168	6,229

Уравнение зависимости доходности отраслевого индекса RTSog (m2) от индекса РТС (mr) имеет вид:

m2=-1,410+ 1,045* mr

Таблица 7

Регрессионная статистика

Множественный R	0,892
R-квадрат	0,795
Нормированный R-квадрат	0,775
Стандартная ошибка	2,860
Наблюдения	12

Таблица 8

Дисперсионный анализ

	df	SS	MS	F	Значимость F
Регрессия	1	317,426	317,426	38,806	0,00
Остаток	10	81,799	8,180		
Итого	11	399,225			

Собственный (несистематический) риск отраслевого индекса RTStl (m1) равен: $\sigma 2\varepsilon 2=\sum \varepsilon 2/ (N-1) = 81,799/11=7,44$, R2=0,50.

Решение оптимизационной задачи

Необходимо найти вектор X= (x1, x2), минимизирующий риск портфеля σp. Решение задачи можно получить в среде Excel с помощью надстройки "Поиск решения".

Экономико-математическая модель задачи

X1 - доля в портфеле отраслевого индекса RTStl

X2 - доля в портфеле отраслевого индекса RTSog

В нашей задаче задана эффективность портфеля не ниже, чем в среднем по облигациям, то есть 0,5% в месяц.

$\sigma p=\sqrt{} (\sum xi\beta i) 2\sigma 2mr+\sum xi\ \sigma 2\varepsilon i=$

$=\sqrt{} (0,3452x12+2*1,045*0,345*x1*x2+1,0452x22) *5,142+14,37x12+7,44\ x22 =>$

=> min;

x1 +x2=1

$mp=\sum xi\ (\alpha i+\beta imr) =x1\ (1,613+0,345*1,59) + x2\ (-1,410+1,045*1,59) \geq 0,5;$

x1; x2≥0

	A	B	C	D	E	F	G	H	I
1	*Решение оптимизационной задачи*								
2					*доли акций*			Целевая функция	
3				*индекс телекоммуникаций*	*индекс нефти и газа*		*риск портфеля*		
4				X1	X2				
5									
6		риск	доход	a	b	собств. риск	рыночн. риск	доля рыночн. риска	
7	*индекс телекоммуникаций*								
8	*индекс нефти и газа*								
9	*рынок*						ограничения		
10					*доли бумаг*				
11					*доход. портф.*				*доход. без риска*
12									
13									

Рис.45. Последовательность решения оптимизационной задачи в среде Excel представлена.

Подготовлена форма для ввода данных.

	A	B	C	D	E	F	G	H	I
1				*Решение оптимизационной задачи*					
2					*доли акций*			Целевая функция	
3				*индекс телекоммуникаций*	*индекс нефти и газа*		*риск портфеля*		
4				X1	X2				
5				0,00%	0,00%				
6		риск	доход	a	b	собств. риск	рыночн. риск	доля рыночн. риска	
7	*индекс телекоммуникаций*	4,18	2,16	1,61	0,34	14,37	3,14	17,91	
8	*индекс нефти и газа*	6,02	0,26	-1,41	1,05	7,44	28,86	79,50	
9	*рынок*	5,14	1,59				ограничения		
10					*доли бумаг*		=	1	
11					*доход. портф.*		>=	0,5	*доход. без риска*
12									
13									

Рис.46. Введение исходных данных: (в ячейках D5 и E5 (эти ячейки называются изменяемыми) будут находиться значения неизвестных X1 и X2)

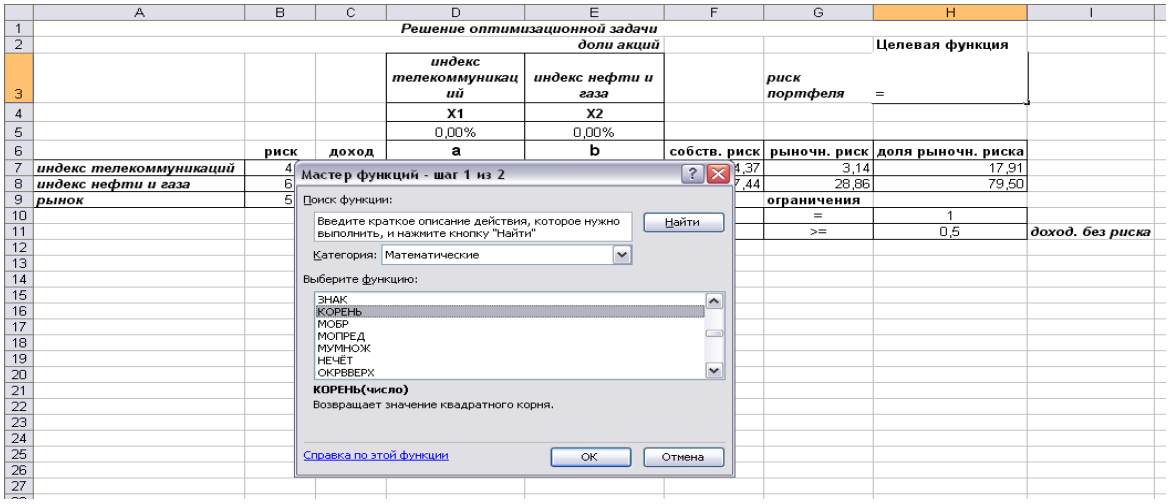


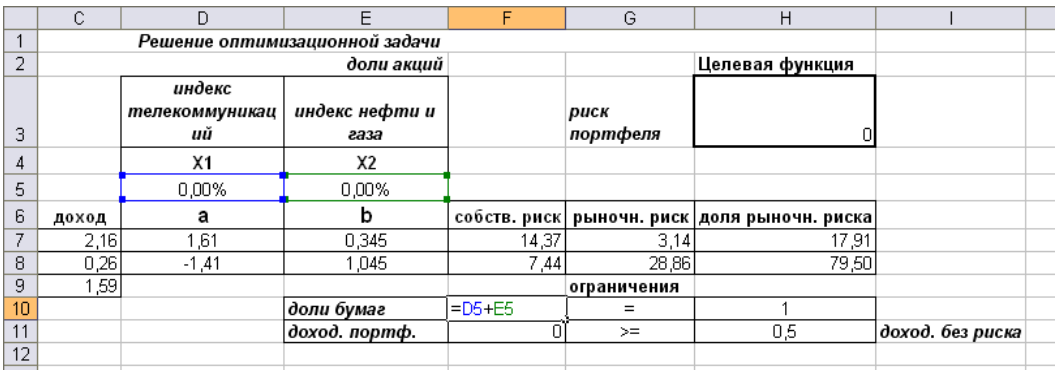
Рис.47. Ввод формулы: (для ввода формулы для расчета целевой функции воспользуемся функцией КОРЕНЬ (шаг 1))

	C	D	E	F	G	H	I	J	K	L
1		*Решение оптимизационной задачи*								
2			*доли акций*			Целевая функция				
3		*индекс телекоммуникаций*	*индекс нефти и газа*		*риск портфеля*	=КОРЕНЬ((E7^2*D5^2+2*E8*D5*E7*E5+E8^2*E5^2)*B9^2+F7*D5^2+F8*E5^2)				
4		X1	X2			КОРЕНЬ(число)				
5		0,00%	0,00%							
6	доход	a	b	собств. риск	рыночн. риск	доля рыночн. риска				
7	2,16	1,61	0,345	14,37	3,14	17,91				
8	0,26	-1,41	1,045	7,44	28,86	79,50				
9	1,59				ограничения					
10			*доли бумаг*		=	1				
11			*доход. портф.*		>=	0,5	*доход. без риска*			
12										
13										

Рис.48. Введение подкоренного выражения (шаг 2.)

	C	D	E	F	G	H	I
1		*Решение оптимизационной задачи*					
2			*доли акций*			Целевая функция	
3		*индекс телекоммуникаций*	*индекс нефти и газа*		*риск портфеля*	0	
4		X1	X2				
5		0,00%	0,00%				
6	доход	a	b	собств. риск	рыночн. риск	доля рыночн. риска	
7	2,16	1,61	0,345	14,37	3,14	17,91	
8	0,26	-1,41	1,045	7,44	28,86	79,50	
9	1,59				ограничения		
10			*доли бумаг*		=	1	
11			*доход. портф.*	=(D7+E7*C9)*D5+(D8+E8*C9)*E5			*доход. без риска*
12							

Рис.49. Введение левой части системы ограничений по доходности портфеля.



	C	D	E	F	G	H	I
1		*Решение оптимизационной задачи*					
2			*доли акций*			Целевая функция	
3		*индекс телекоммуникаций*	*индекс нефти и газа*		*риск портфеля*	0	
4		X1	X2				
5		0,00%	0,00%				
6	доход	a	b	собств. риск	рыночн. риск	доля рыночн. риска	
7	2,16	1,61	0,345	14,37	3,14	17,91	
8	0,26	-1,41	1,045	7,44	28,86	79,50	
9	1,59				ограничения		
10			*доли бумаг*	=D5+E5	=	1	
11			*доход. портф.*	0	>=	0,5	*доход. без риска*
12							

Рис.50. Введение левой части системы ограничений по долям бумаг.

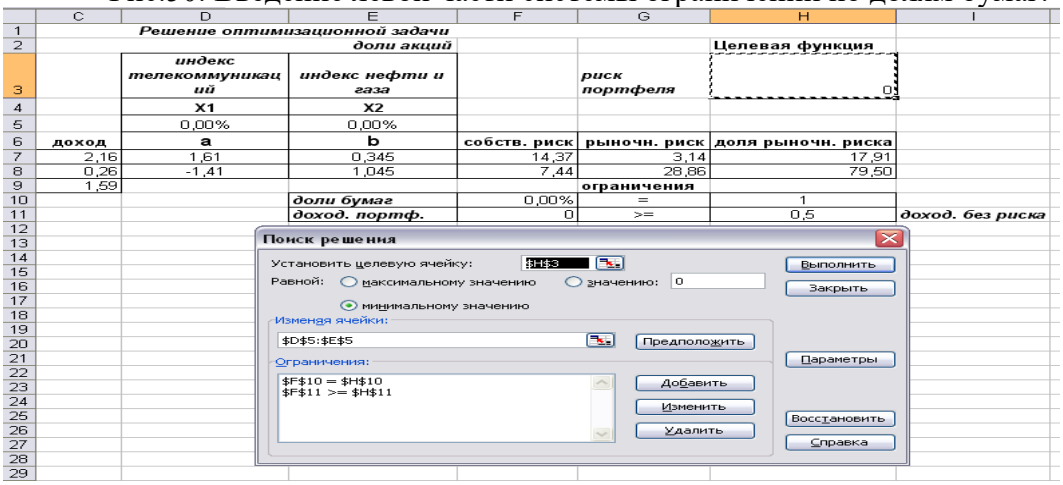


Рис.51. Указание целевой ячейки (H3), изменяемых ячеек (D6: 5E)

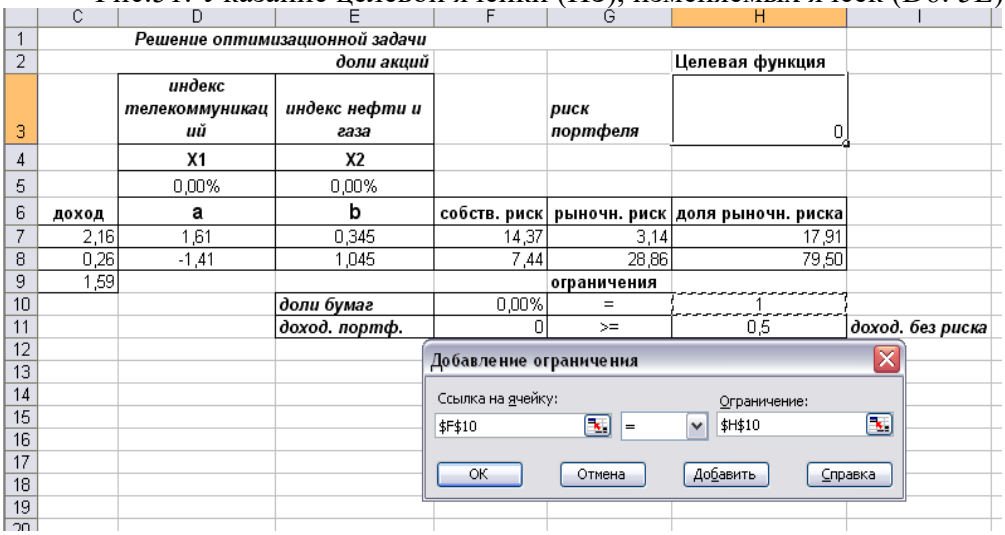


Рис.52. Добавление ограничений.

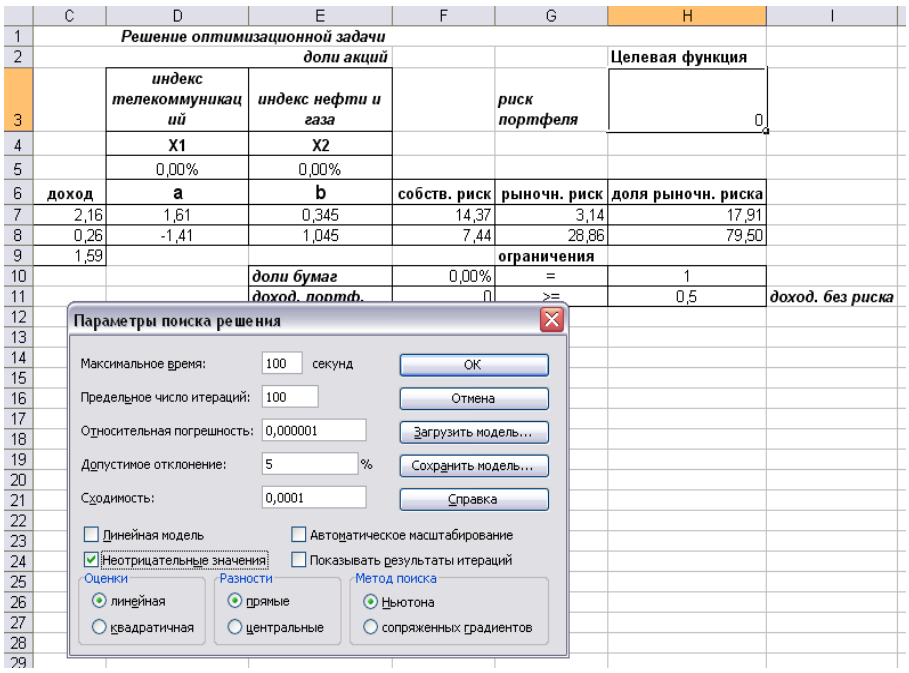


Рис.53. Указание параметров.

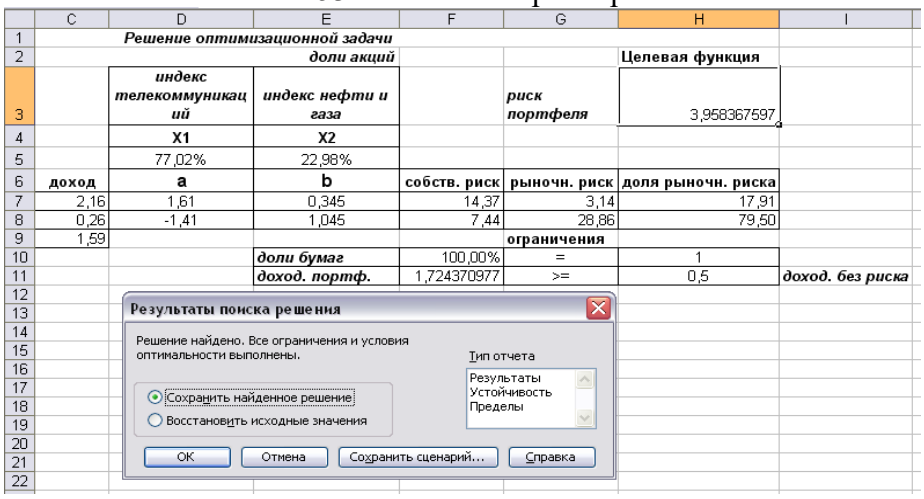


Рис.54. Решение найдено.

Ответ. Минимальный риск портфеля, равный 3,96%, будет достигнут, если доля отраслевого индекса телекоммуникаций (RTStl) составит77,02%, а доля отраслевого индекса нефти и газа (RTSog) - 22,98%.

ЛАБОРАТОРНАЯ РАБОТА № 8
Количественный анализ риска инвестиционных проектов

Задание:

Алгоритма имитационного моделирования (инструмент “РИСК-АНАЛИЗ”):

1.Определить ключевые факторы ИП.

Для этого предлагается применять анализ чувствительности по всем факторам (цена реализации, рекламный бюджет, объём продаж, себестоимость продукции и т. д.), используя специализированные пакеты типа Project Expert и Альт-Инвест, что позволит существенно сократить время расчётов. В качестве ключевых выбираются те факторы, изменения которых приводят к наибольшим отклонениям чистой текущей стоимости (NPV).

Таблица 9

Выбор ключевых факторов ИП на основе анализа чувствительности

Факторы	-20%	-10%	0	10%	20%	Дисперсия NPV
F_1	npv_{11}	npv_{12}	npv_{13}	npv_{14}	npv_{15}	Var (npv_1)
F_2	npv_{21}	npv_{22}	npv_{23}	npv_{24}	npv_{25}	Var (npv_2)
F_3	npv_{31}	npv_{32}	npv_{33}	npv_{34}	npv_{35}	Var (npv_3)
F_4	npv_{41}	npv_{42}	npv_{43}	npv_{44}	npv_{45}	Var (npv_4)
F_5	npv_{51}	npv_{52}	npv_{53}	npv_{54}	npv_{55}	Var (npv_5)
…						
F_n	npv_{n1}	npv_{n2}	npv_{n3}	npv_{n4}	npv_{n5}	Var (npv_n)

2. Определить максимальное и минимальное значения ключевых факторов, и задаётся характер распределения вероятностей. В общем случае рекомендуется использовать нормальное распределение.

3. На основе выбранного распределения провести имитацию ключевых факторов, с учётом полученных значений рассчитываются значения NPV.

4. На основе полученных в результате имитации данных рассчитать критерии, количественно характеризующие риск ИП (матожидание NPV, дисперсия, среднеквадратическое отклонение и др.).

5. Для проведения сценарного анализа воспользоваться методикой, позволяющей учитывать все возможные сценарии развития, а не три варианта (оптимистичный, пессимистичный, реалистичный). Предлагается следующий алгоритм сценарного анализа.

Алгоритм сценарного анализа:

1.Используя анализ чувствительности, определяются ключевые факторы ИП (см. выше).

2.Рассматриваются возможные ситуации и сочетания ситуаций, обусловленные колебаниями этих факторов. Для этого рекомендуется строить “дерево сценариев”.

3.Методом экспертных оценок определяются вероятности каждого сценария.

4.По каждому сценарию с учетом его вероятности рассчитывается NPV проекта, в результате чего получается массив значений NPV (табл. 10.).

Таблица 10

Массив значений NPV

Сценарий	1	2	3	4	5	…	n
Вероятность	P_1	P_2	P_3	P_4	P_5	…	P_n
NPV	npv_1	npv_2	npv_3	npv_4	npv_5	…	npv_n

5. На основе данных массива рассчитываются критерии риска ИП

Ход решения:

Моделируя значение NPV в зависимости от ключевых факторов были получены значения NPV по трём опорным вариантам развития событий (оптимистичный, пессимистичный, реалистичный). Методом экспертных оценок были определены также вероятности реализации этих вариантов. Полученные результаты использовались как исходные данные для имитационного моделирования (табл. 11.).

Таблица 11

Исходные условия эксперимента

	NPV (тыс. руб.)	Вероятность
Минимум	9634	0,05
Вероятное	14790	0,9
Максимум	43163	0,05

На основе исходных данных проводим имитацию. Для проведения имитации рекомендуется использовать функцию “Генерация случайных чисел” (рис. 1)

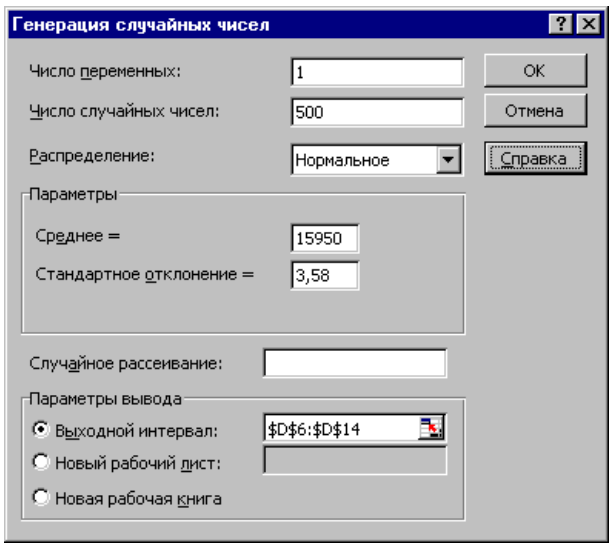


Рис.55. Имитация с использованием генерации случайных чисел.

Для осуществления имитации рекомендуется использовать нормальное распределение, так как практика риск-анализа показала, что именно оно встречается в подавляющем большинстве случаев. Количество имитаций может быть сколь угодно большим и определяется требуемой точностью анализа. В данном случае ограничимся 500 имитациями.

Таблица 12

Имитация

№ п.п.	NPV (тыс.р.)
1	15940,14853
2	15951,41663
3	15947,78512
4	15953,94136
5	15951,61013
6	15950,67133
7	15949,48875
8	15955,30642
9	15954,1289
10	15953,20001
…	…

На основе полученных в результате имитации данных, используя стандартные функции MS Excel проводим экономико-статистический анализ (рис. 56).

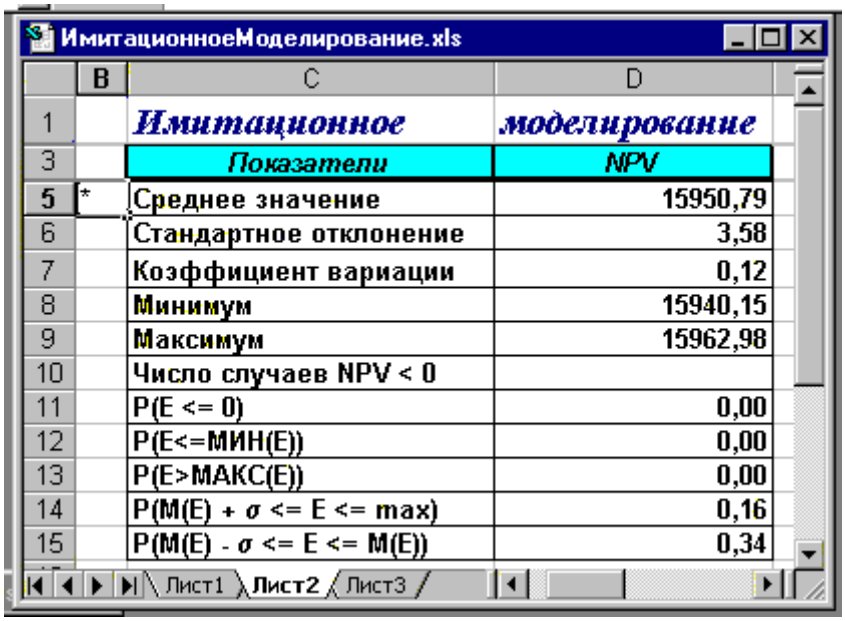


Рис. 56. Экономико-статистический анализ результатов имитации

Имитационное моделирование продемонстрировало следующие результаты:

1. Среднее значение NPV составляет 15950,79 тыс. руб.
2. Минимальное значение NPV составляет 15940,15 тыс. руб.
3. Максимальное значение NPV составляет 15962,98 тыс. руб.
4. Коэффициент вариации NPV равен 12%
5. Число случаев NPV < 0 – нет.
6. Вероятность того, что NPV будет меньше нуля равна нулю.
7. Вероятность того, что NPV будет больше максимума также равна нулю.
8. Вероятность того, что NPV будет находится в интервале [M(E) + s ; max] равна 16%.
9. Вероятность того, что NPV будет находиться в интервале [M(E) - s ; [M(E)] равна 34%

Оценим риск данного инвестиционного проекта.

Для расчёта цены риска в данном случае используем показатель среднеквадратического отклонения - s , и матожидания – M (NPV). В соответствии с правилом “трёх сигм”, значение случайной величины, в данном случае – NPV, с вероятностью близкой 1 находится в интервале [M-3s ; M+3s]. В экономическом контексте это правило можно истолковать следующим образом:

- вероятность получить NPV проекта в интервале [15950,79-3,58 ; 15950,79 +3,58] равна 68%;
- вероятность получить NPV проекта в интервале [15950,79-7,16 ; 15950,79 +7,16] равна 94%;
- вероятность получить NPV проекта в интервале [15950,79-10,74 ; 15950,79 +10,74] близка к единице, т.е. вероятность того, что значение NPV проекта будет ниже 15 940,05 тыс. руб. (15950,79-10,74) стремится к нулю.

Таким образом, суммарная величина возможных потерь характеризующих данный инвестиционный проект, составляет 10,74 тыс. руб. (что позволяет говорить о высокой степени надёжности проекта).

Иначе говоря, цена риска данного ИП составляет 10,74 тыс. рублей условных потерь, т.е. принятие данного инвестиционного проекта влечёт за собой возможность потерь в размере не более 10,74 тыс. руб.

Риск-анализ инвестиционного проекта методом сценариев

Для сравнения проведём риск-анализ того же инвестиционного проекта методом сценариев. Рассмотрим возможные сценарии реализации инвестиционного проекта. В данном случае их будет только три:

Таблица 13

Исходные данные

Сценарии	Наилучший	Вероятный	Наихудший
Вероятности	0,05	0,9	0,05
Тариф (руб.)	370	187,9	187,9
Себестоимость(руб.)	95,40	53,37	81.73
NPV(руб.)	43163,00	14790,00	9634,00

Построение сценариев и расчёт NPV по вариантам осуществлялся с учетом того факта, что себестоимость 1Гкал, вырабатываемой локальной котельной и тариф за централизованное отопление в значительной степени коррелируют друг с другом, поскольку обе эти величины зависят от одних и тех же факторов, как то эксплуатационные расходы и зарплата обслуживающего персонала.

Экономико-статистический анализ данных метода сценариев показан на рис.57.

	A	B	C	D
3	**Анализ сценариев**			
4	**Сценарии**	**Наилучший**	**Вероятный**	**Наихудший**
6	Вероятности	0,05	0,9	0,05
7	Тариф	370	187,9	187,9
8	Себестоимость	95,40	53,37	81.73
9	NPV	43163,00	14790,00	9634,00
10	Средняя *NPV*	15950,85		
11	Квадраты разностей	740501107,62	1347572,72	39902593,92
12	Отклонение σ	6342,95		
13	Коэф. вариации *CV*	0,40		
14	*P(NPV<=0)*	0,01		
15	*P(NPV<=Среднее)*	=НОРМРАСП(Среднее*0,5;Среднее;Отклонение;1)		
16	*P(NPV>максимума)*	0,00		
17	*P(NPV>Среднее + 10%)*	0,40		
18	*P(NPV>Среднее + 20%)*	0,31		
19				
20				
21				

Лист1 Лист2 Лист3

Рис. 57. Экономико-статистический анализ данных метода сценариев

Сценарный анализ продемонстрировал следующие результаты:

1. Среднее значение NPV составляет 15950,85 руб.
2. Коэффициент вариации NPV равен 40 %.
3. Вероятность того, что NPV будет меньше нуля 1 %.
4. Вероятность того, что NPV будет больше максимума равна нулю.
5. Вероятность того, что NPV будет больше среднего на 10 % равна 40 %.
6. Вероятность того, что NPV будет больше среднего на 20 % равна 31%.

Анализируя полученные результаты, отмечаем, что метод сценариев даёт более пессимистичные оценки относительно риска инвестиционного проекта. В частности коэффициент вариации, определённый по результатам этого метода значительно больше, чем в случае с имитационным моделированием.

Рекомендуется использовать сценарный анализ только в тех случаях, когда количество сценариев конечно, а значения факторов дискретны. Если же количество сценариев очень велико, а значения факторов непрерывны, рекомендуется применять имитационное моделирование.

Следует отметить, что, используя сценарный анализ можно рассматривать не только три варианта, а значительно больше. При этом можно сочетать сценарный анализ с другими

методами количественного анализа рисков, например, с методом дерева решений и анализом чувствительности, как это продемонстрировано в следующем примере.

Анализ рисков бизнес-плана ТК "Корона". Установим ключевые факторы проекта, оказывающие значительное влияние на показатель эффективности – NPV. Для этого проведём анализ чувствительности по всем факторам в интервале от –20% до +20% и выберем те из них, изменения которых приводят к наибольшим изменениям NPV (рис. 58)

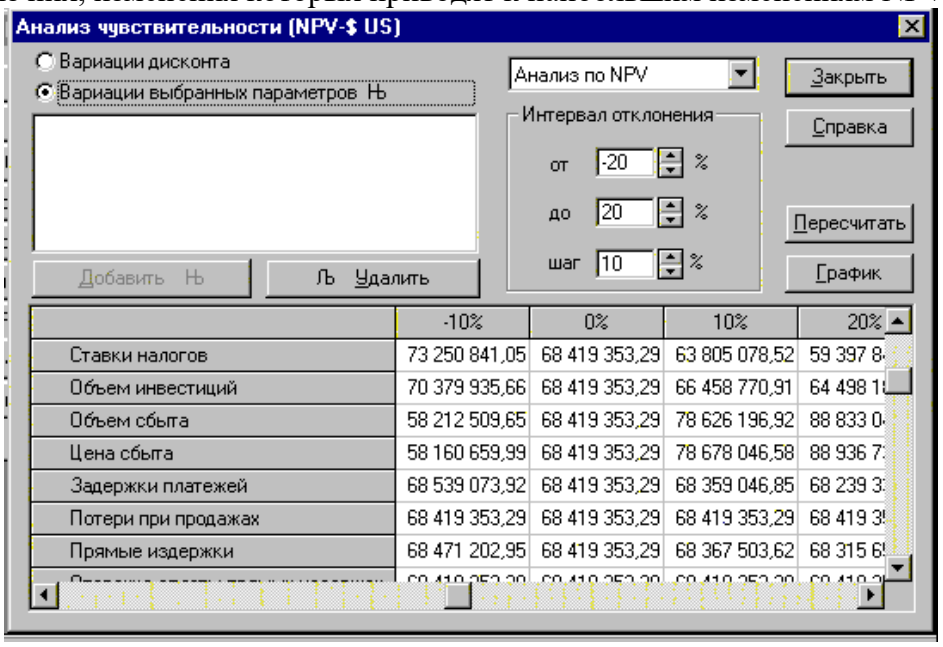


Рис. 58. Анализ чувствительности в Project Expert

В нашем случае это факторы: ставки налогов; объём сбыта, цена сбыта.

Рассмотрим возможные ситуации, обусловленные колебаниями этих факторов. Для этого построим "дерево сценариев".

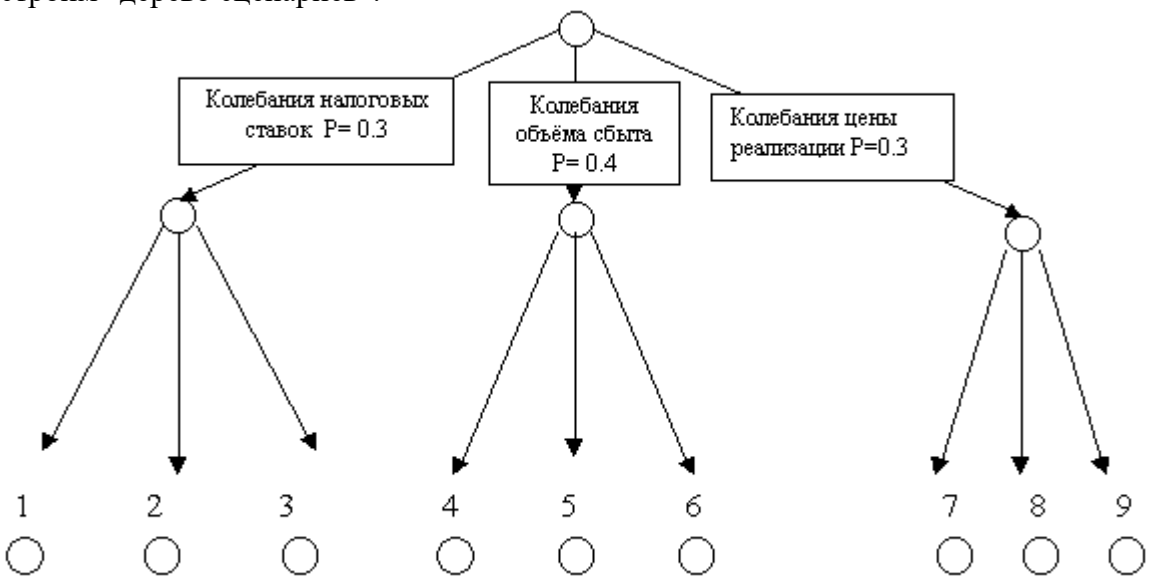


Рис. 59. Дерево сценариев

Ситуация 1: Колебания налоговых ставок Вероятность ситуации = 0,3

Ситуация 2: Колебания объёма сбыта Вероятность ситуации = 0,4

Ситуация 3: Колебания цены сбыта Вероятность ситуации = 0,3

Рассмотрим также возможные сценарии развития этих ситуаций.

Ситуация 1: Колебания налоговых ставок

Вероятность ситуации = 0,3

Сценарий 1: Снижение налоговых ставок на 20%

Вероятность сценария в рамках данной ситуации = 0,1

Общая вероятность сценария =0,1* 0,3=0,03

Сценарий 2: Налоговые ставки остаются неизменными

Вероятность сценария в рамках данной ситуации = 0,5

Общая вероятность сценария =0,5* 0,3=0,15

Сценарий 3: Повышение налоговых ставок на 20%

Вероятность сценария в рамках данной ситуации = 0,4

Общая вероятность сценария =0,4* 0,3=0,12

Ситуация 2: Колебания объёма реализации Вероятность ситуации = 0,4

Сценарий 4: Снижение объёма реализации на 20% P=0,25* 0,4=0,1

Сценарий 5: Объёма реализации не изменяется P=0, 5* 0,4=0,2

Сценарий 6: Увеличение объёма реализации на 20% P=0,25* 0,4=0,1

Ситуация 3: Колебания цены реализации Вероятность ситуации = 0,3

Сценарий 7: Снижение цены реализации на 20% P=0,2* 0,3=0,06

Сценарий 8: Цена реализации не изменяется P=0, 5* 0,3=0,15

Сценарий 9: Увеличение цены реализации на 20% P=0,3* 0,3=0,09

По каждому из описанных сценариев определяем NPV (эти значения были рассчитаны при анализе чувствительности), подставляем в таблицу и проводим анализ сценариев развития.

Таблица 14

Ситуация 1

Ситуация		1	
Сценарии	1	2	3
Вероятности	0,03	0,15	0,12
NPV	78 310 414	68 419 353	59 397 846

Таблица 15

Ситуация 2

Ситуация		2	
Сценарии	4	5	6
Вероятности	0,1	0,2	0,1
NPV	48 005 666	68 419 353	88 833 040

Таблица 16

Ситуация 3

Ситуация		3	
Сценарии	7	8	9
Вероятности	0,06	0,15	0,09
NPV	47 901 966	68 419 353	88 936 739

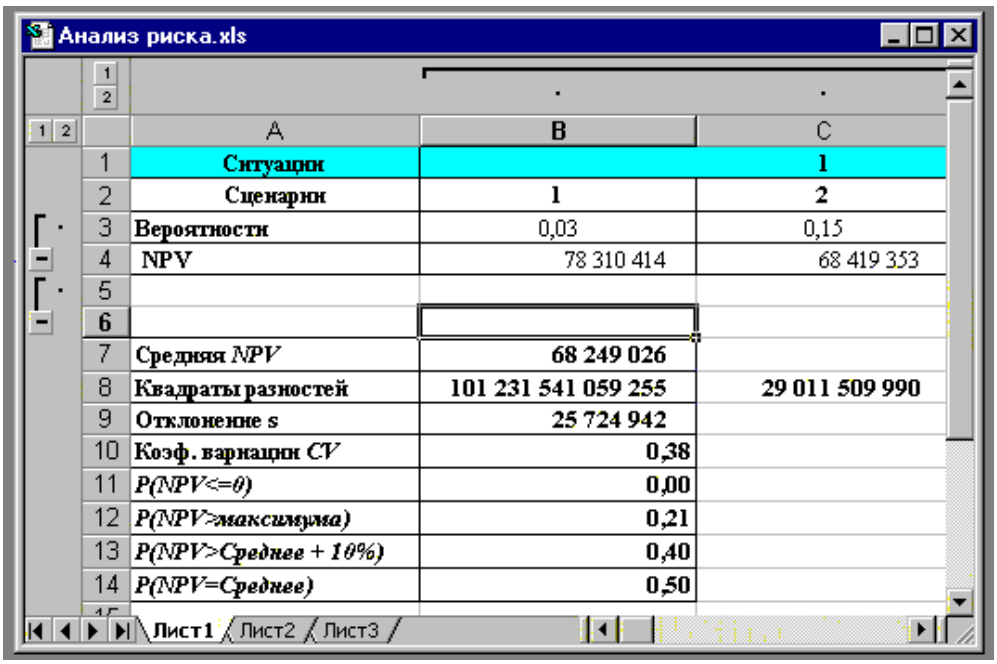


Рис. 60. Итоговая таблица сценарного анализа

Проведённый риск-анализ проекта позволяет сделать следующие выводы:

1. Наиболее вероятный NPV проекта (68 249 026 тыс. руб.) несколько ниже, чем ожидают от его реализации (68 310 124 тыс. руб.)

2.Несмотря на то, что вероятность получения NPV меньше нуля равна нулю, проект имеет достаточно сильный разброс значений показателя NPV, о чем говорят коэффициент вариации и величина стандартного отклонения, что характеризует данный проект как весьма рискованный. При этом несомненными факторами риска выступают снижение объёма и цены реализации.

3. Цена риска ИП в соответствии с правилом “трёх сигм” составляет 3* 25 724 942 = 77 174 826 тыс. руб., что превышает наиболее вероятный NPV проекта (68 249 026 тыс. руб.)

Цену риска можно также охарактеризовать через показатель коэффициент вариации (CV). В данном случае CV = 0,38. Это значит, что на рубль среднего дохода (NPV) от ИП приходится 38 копеек возможных потерь с вероятностью равной 68%.. Эффективность применения разработанных авторами технологий инвестиционного проектирования обусловлена тем, что они могут быть легко реализованы обычным пользователем ПК в среде MS Excel, а универсальность математических алгоритмов, используемых в технологиях, позволяет применять их для широкого спектра ситуаций неопределённости, а также модифицировать и дополнять другими инструментами.

Практика применения предлагаемого инструментария в Нижегородской области продемонстрировала его высокую надежность и перспективность. Экономический эффект от внедрения новых проектных технологий выражается в снижении размера резервных фондов и страховых отчислений, необходимость которых обусловлена наличием рисков и неопределённостью условий реализации проекта. Опыт применения данных алгоритмов может найти широкое применение во всех регионах России и быть использован как для проектирования ИП предприятий, независимо от их форм собственности и отраслевой принадлежности, так и финансовыми учреждениями для анализа эффективности этих проектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Енина Е.П. Лаврёнова Г.А.Управление рисками и страхование. Ч. 1: Управление рисками: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (4.0 Мб) / Е.П. Енина Г.А. Лаврёнова, Воронеж: ФГБОУ ВО «Воронежский государственный технический университет», 2016. – 1 электрон. опт. диск (CD-ROM). цв. – Систем. требования: ПК 500 и выше; 256 Мб ОЗУ ; Windows XP ; SVGA с разрешением 1024x768 ; Adobe Acrobat; CD-ROM дисковод ; мышь. – Загл. с экрана.

2 Балдин, К.В.Управление рисками в инновационно-инвестиционной деятельности : учебное пособие [Электронный ресурс] : учеб. пособие / К.В. Балдин, И.И. Передеряев, Р.С. Голов. — Электрон. дан. — Москва : Дашков и К, 2017. — 418 с. — Режим доступа: https://e.lanbook.com/book/93406. — Загл. с экрана.

3 Балдин, К.В.Управление рисками [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по специальностям экономики и управления (060000) / К.В. Балдин, С.Н. Воробьев. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 511 с. — 5-238-00861-9. — Режим доступа: http://www.iprbookshop.ru/71229.html

4Поздеева С.Н.Основы управления рисками [Электронный ресурс] : практикум / С.Н. Поздеева. — Электрон. текстовые данные. — М. : Российская таможенная академия, 2016. — 68 с. — 978-5-9590-0927-4. — Режим доступа: http://www.iprbookshop.ru/69984.html

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Методические указания к проведению лабораторных работ по дисциплине «Оценка рисков» для студентов специальности 38.05.01 «Экономическая безопасность»/ ФГБОУ ВО «Воронежский государственный технический университет»; сост.: Е.П. Енина, И.А. Шишкин. – Воронеж: ВГТУ, 2018. 58с.

Составители:
Е.П.Енина, И.А.Шишкин

Подписано к изданию 2018.

Уч.-изд. л.

ФГБОУ ВО «Воронежский государственный технический университет»

394026 Воронеж, Московский просп., 14