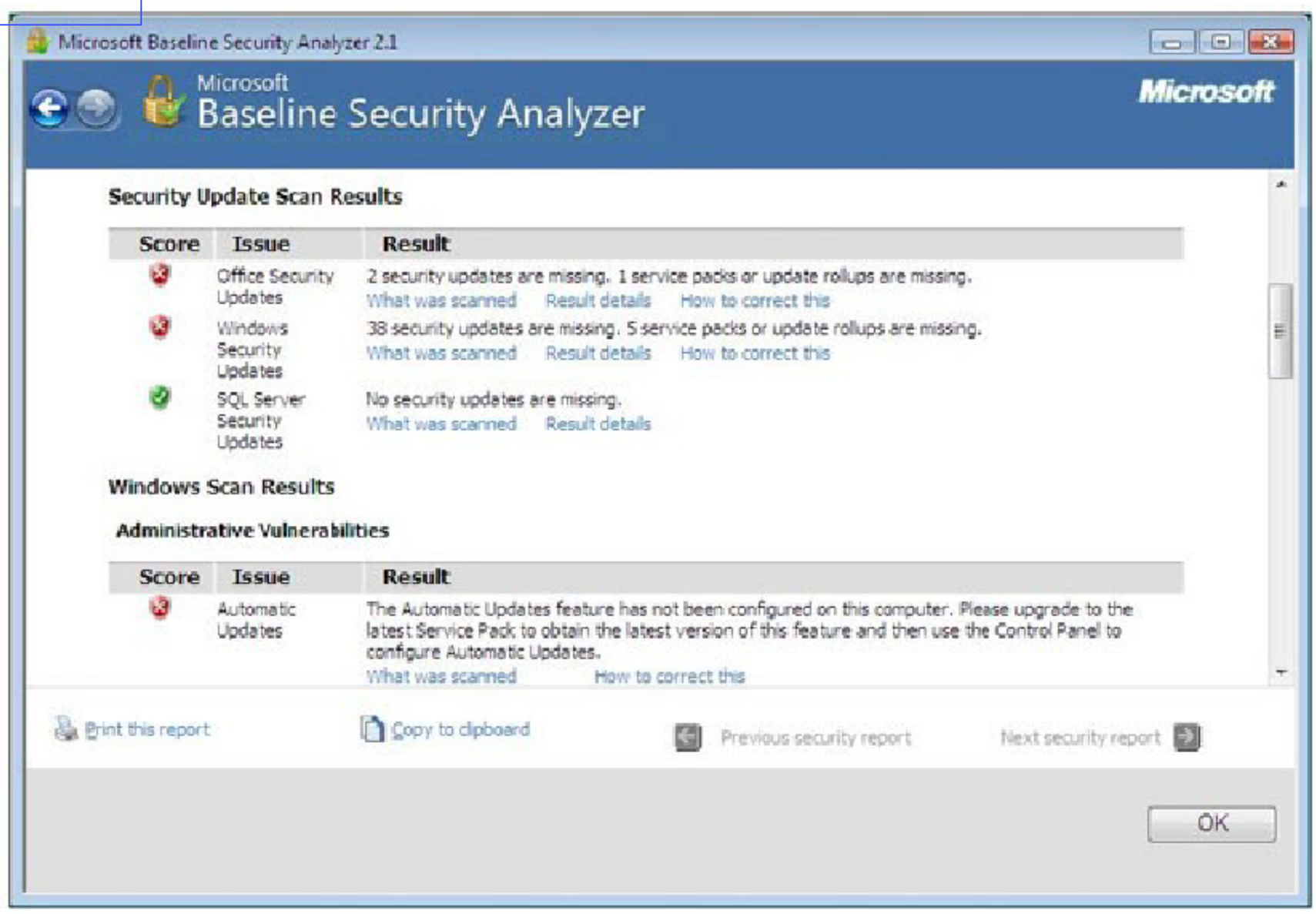

Рис. 5.4. Перечень неустановленных обновлений (по группам)

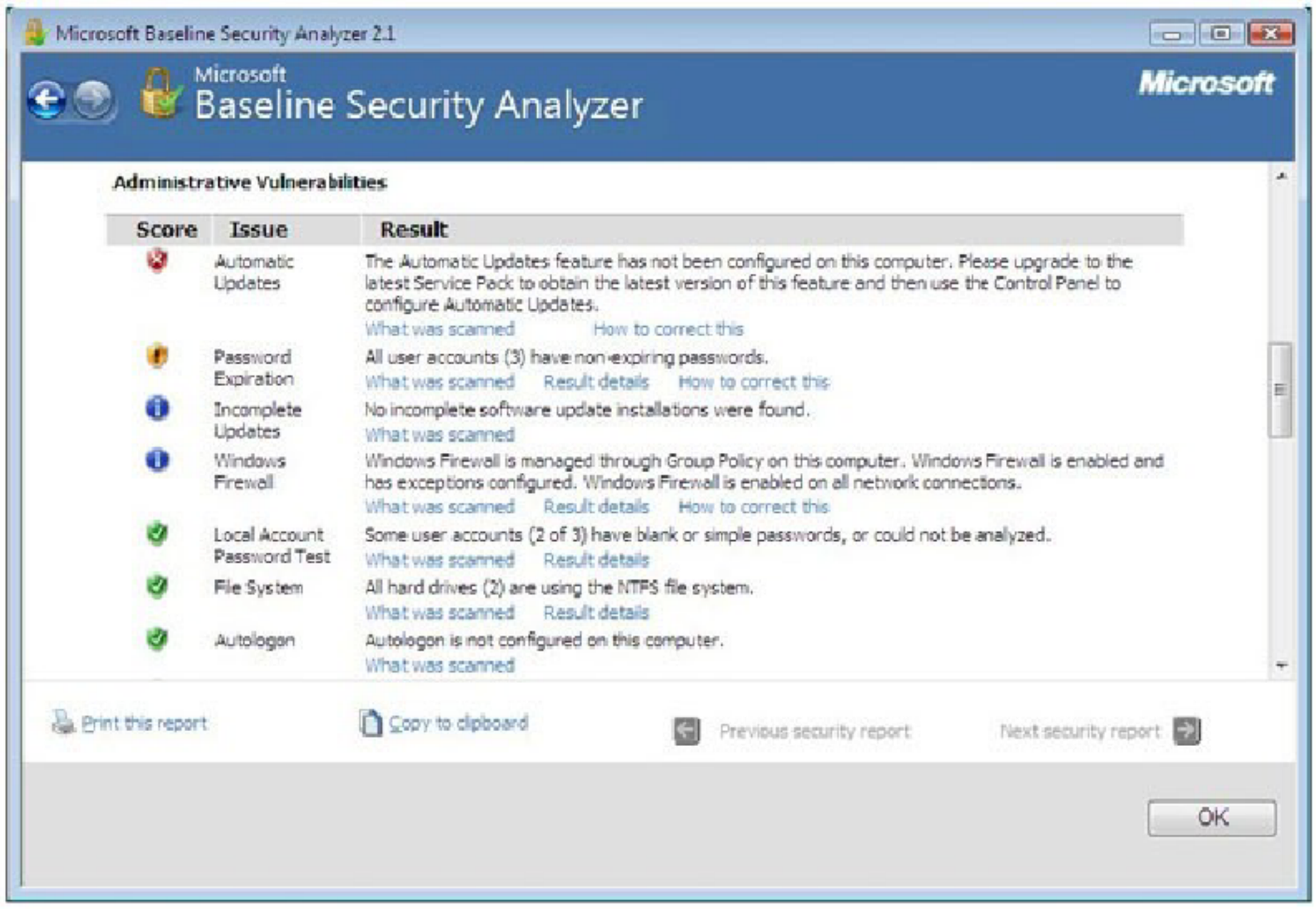

Рис. 5.5. Уязвимости, связанные с администрированием операционной системы

Аналогичным образом проводится работа *по* анализу других групп уязвимостей (рис. 5.5). Описывается *уязвимость*, указывается ее уровень критичности, даются рекомендации *по* исправлению. На рис. 5.6 представлено подробное описание результатов (*ссылка* **result details**) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные *по* сроку действия.

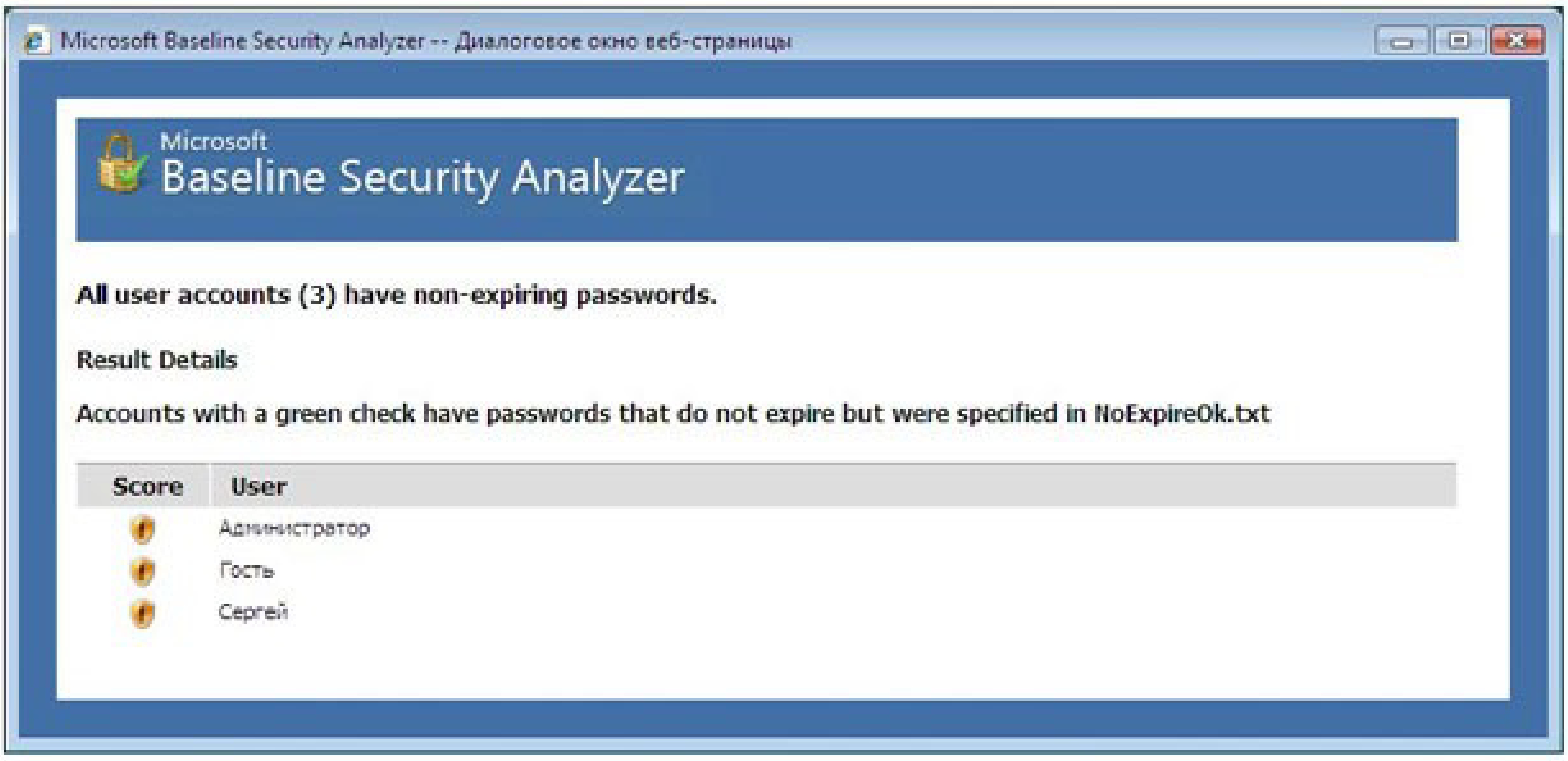

Рис. 5.6. Результаты проверку паролей

Кроме версии программы с графическим интерфейсом, существует также *утилита* с интерфейсом командной строки. Называется она mbsacli.exe и находится в том же каталоге, куда устанавливался *Baseline security analyzer*, например, **"C:\Program Files\ Microsoft Baseline Security Analyzer 2"**. У утилиты есть достаточно много ключей, получить информацию о которых можно запустив ее с ключом **"/?"**.

Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на *консоль*. Чтобы сохранить результаты сканирования, можно перенаправить *вывод* в какой-либо *файл*. Например: mbsacli > mylog.txt. Хотелось бы еще раз обратить внимание на то, что при настройках *по* умолчанию сначала *утилита* обращается на *сайт* Майкрософт за информацией об обновлениях. Если соединение с *Интернет* отсутствует, то утилиту надо запускать или с ключом /nd (указание "не надо скачивать файлы с сайта Майкрософт") или с ключом/n Updates (указание "не надо проводить проверку обновлений").

Запуск с ключом /xmlout приводит к запуску утилиты в режиме проверки обновлений (т.е. проверка на уязвимости, явившиеся результатом неудачного администрирования, проводиться не будет), при этом, отчет формируется в формате xml. Например:

mbsacli /xmlout > c:\myxmlog.xml

Задания

1. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении лабораторной укажите:

   - как оценен уровень уязвимости Вашего компьютера;
   - какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
   - опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.

2. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

3. Теперь выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или IP-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате Вы получите сообщение примерно следующего содержания:

4. Computer Name, IP Address, Assessment, Report Name

5. HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. *Вывод* можно перенаправить в *текстовый файл* для дальнейшей обработки. Например:

mbsacli/ld "HOME - MYNBOOK (06.12.2008 13-51)" > c:\test\report1.txt

После выполнения задания проанализируйте результаты, кратко опишите их в отчете *по* практической работе.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-3	1-2	1-3

Оценочные средства: собеседование.

3.6.ПРАКТИЧЕСКАЯ РАБОТА 6. Настройка локальной политики парольной безопасности операционной системы.

Цель работы:

Изучить методы повышения надежности путем практического применения рекомендаций по администрированию парольной системы операционной системы.

Содержание:

Администрирование парольной системы. Локальная политика безопасности операционной системы. Свойства учетных записей. Политика паролей и учетных записей. Особенности простых и групповых учетных записей.

Теоретический материал.

Локальная политика паролей. Рассмотрим теперь, какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. В теоретической части курса мы рассматривали рекомендации *по* администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка делается через **Панель управления Windows**.

Откройте **Панель управления** ⟶ **Администрирование** ⟶ **Локальная политика безопасности**. Выберите в списке **Политика учетных записей** и **Политика паролей**. Для *Windows* Vista экран консоли управления будет выглядеть так, как представлено на рис. 1.

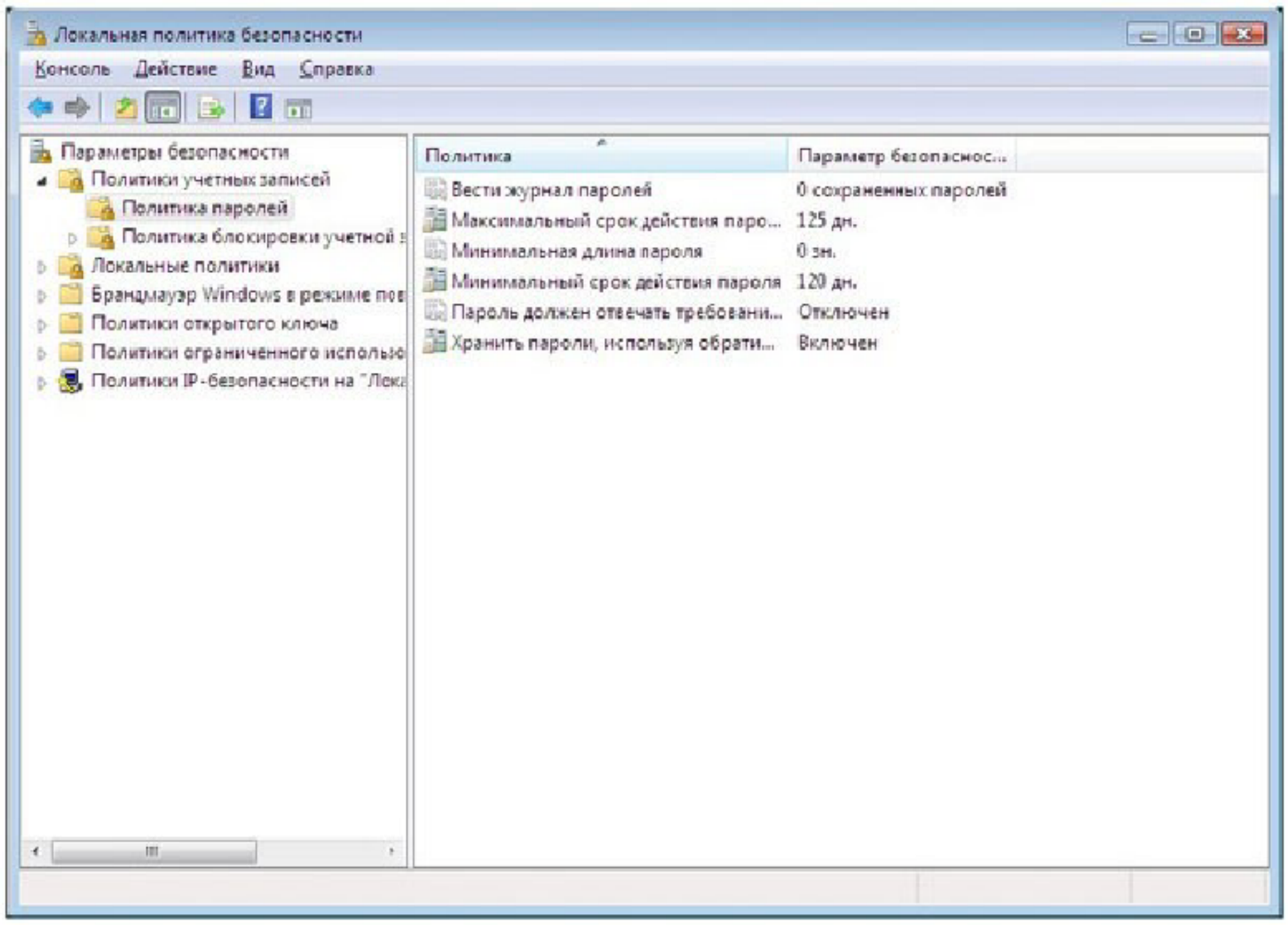

Рис. 1. Настройка политики паролей

Значения выбранного параметра можно изменить (рис. 2). Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться. Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в

учебном классе нужна "групповая" учетная *запись*, параметры которой известны всем студентам, лучше поставить для нее **"Срок действия пароля не ограничен"** и **"Запретить смену пароля пользователем"**.

Свойства учетной записи можно посмотреть в **Панель управления** ⟶ **Администрирование** ⟶ **Управление компьютером**, там выберите **Локальные пользователи и группы** и **Пользователи** (или запустив эту же оснастку через **Пуск** ⟶ **Выполнить** ⟶ **lusrmgr.msc**).

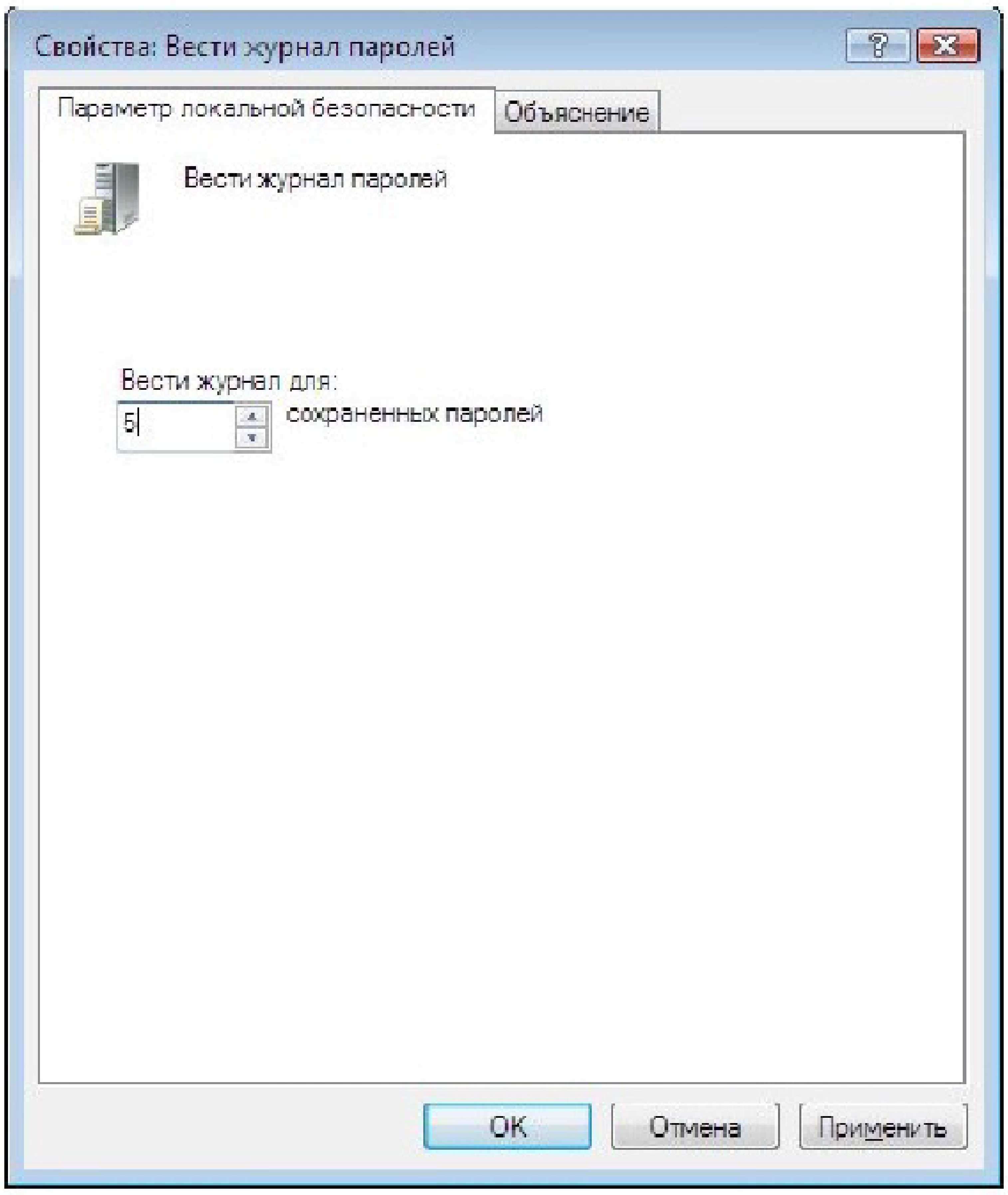

Рис. 2. Установка требования ведения журнала паролей

Задания

1. Опишите действующую на вашем компьютере политику паролей.

2. Измените ее в соответствии с рассмотренными в теоретической части курса рекомендациями по администрированию парольной системы.

Если в ходе проверки утилитой *bsa* были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Контрольные вопросы:

1. Что такое политика парольной безопасности?
2. Локальная политика безопасности операционной системы.
3. Администрирование парольной системы..
4. Свойства учетной записи.
5. Особенности простых и групповых учетных записей.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-3	1-2	1-3

Оценочные средства: собеседование.

3.7.ПРАКТИЧЕСКАЯ РАБОТА 7. Инфраструктура открытых ключей. Цифровые сертификаты.

Цель работы:

Изучить инфраструктуру открытых ключей и цифровые сертификаты.

Содержание:

Инфраструктура открытых ключей (*Public* Key *Infrastructure*, сокр. *PKI*). Центры распределения ключей. Цифровые сертификаты. Проблема аутентификации ключа. Криптографический протокол. Атака типа "человек посередине" (*man* in the middle). Структура PKI. Иерархия центров сертификации и клиентов. Сертификат формата X.509 v.3. Структура списка отозванных сертификатов.

Теоретический материал.

Как было рассмотрено ранее, использование протокола Kerberos позволяет провести аутентификацию и распределить ключи симметричного шифрования. Использование методов асимметричной криптографии сделало возможным безопасный обмен *криптографическими ключами* между отправителем и получателем без использования *центров распределения ключей*.

Но возникает другая проблема - как убедиться в том, что имеющийся у Вас открытый *ключ* другого абонента на самом деле принадлежит ему. Иными словами, возникает проблема аутентификации ключа. Без этого, на криптографический протокол может быть осуществлена *атака* типа "человек посередине" (*man* in the middle).

Идею данной атаки поясняет следующий пример. *Абонент* А (Алиса) хочет послать абоненту В (Боб) зашифрованное сообщение и берет его открытый *ключ* из общедоступного справочника.

Но, на самом деле, ранее нарушитель Е (Ева) подменил в справочнике открытый *ключ* Боба своим открытым ключом. Теперь Ева может расшифровать те сообщения, которые Алиса формирует для Боба, ознакомиться с их содержимым, возможно, зашифровать их на настоящем ключе Боба и переслать ему (рис. 1).

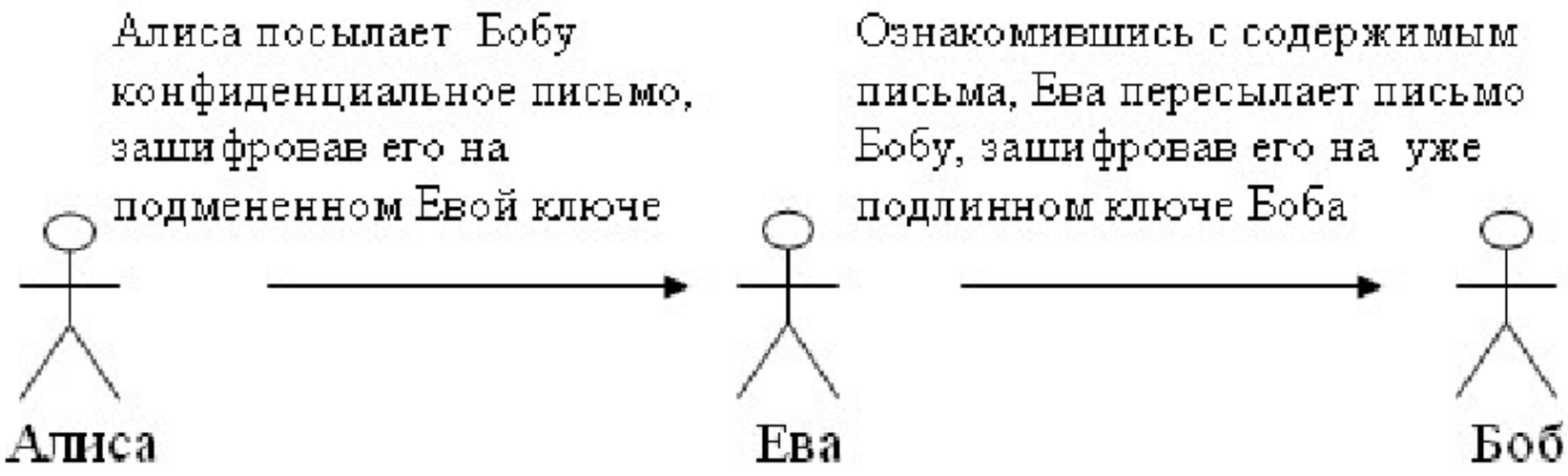

Рис. 1. Атака типа man-in-the-middle

Избежать подобной атаки можно, подтвердив подлинность используемого ключа. Но Алиса и Боб лично никогда не встречались, и передать, например, дискету с ключом из рук в руки не могут. Поэтому, решение задачи подтверждения подлинности берет на себя *третья доверенная сторона* - некий арбитр, которому доверяют оба абонента. Заверяется *ключ* с помощью цифрового сертификата.

На самом деле, подобный способ применяется и вне компьютерных систем. Когда для подтверждения подлинности человека используется паспорт, то в роли третьей

доверенной стороны выступает государство (от имени которого действовали в выдавшем паспорт отделе милиции).

Но вернемся к цифровым сертификатам. Для подтверждения подлинности открытых ключей создается *инфраструктура открытых ключей* (англ. *Public* Key *Infrastructure*, сокр. *PKI*). *PKI* представляет собой набор средств, мер и правил, предназначенных для управления ключами, политикой безопасности и обменом защищенными сообщениями. Структура *PKI* представлена на рис. 2.

Для простоты последующего изложения, будем представлять *сеть* в виде совокупности *удостоверяющих центров* (другое название - *центр сертификации*, от англ. *Certification Authority*, сокр. - *CA*) и пользователей. *Центр сертификации* - *абонент*, которому доверено право удостоверять своей подписью сертификаты, связывающие открытые ключи абонентов с их идентификационной информацией. Сами *центры сертификации* тоже получают сертификаты своих ключей у центров более высокого уровня.

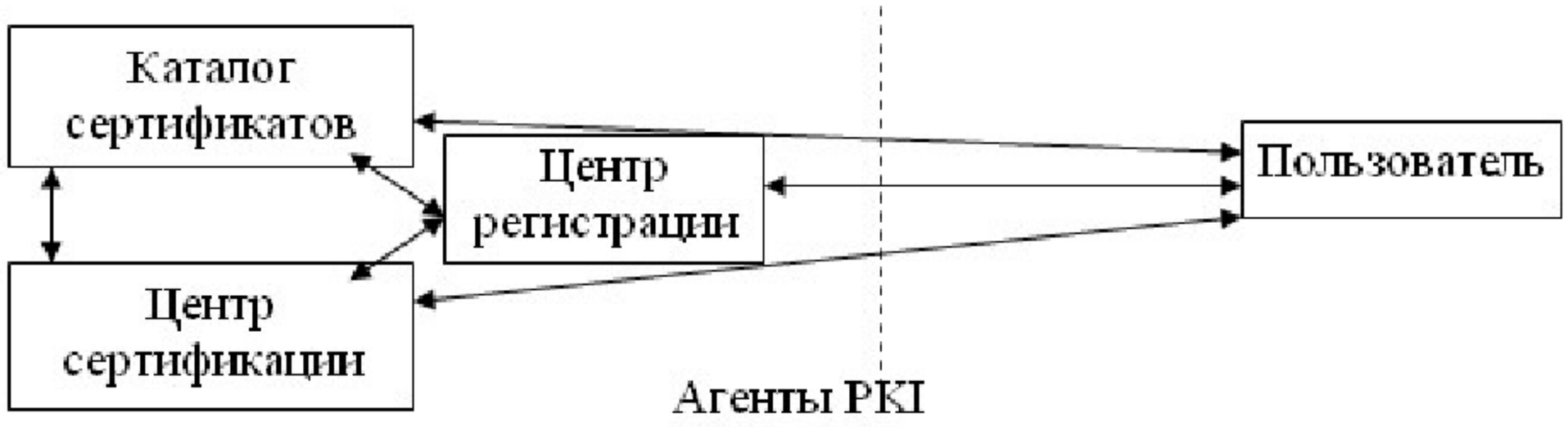

Рис. 2. Структура PKI

Таким образом, *центры сертификации* и пользователи формируют древовидную иерархическую структуру (рис. 3). В вершине этого дерева находится корневой *центр сертификации*, на рисунке - CA_1. Его особенность заключается в том, что он использует *самоподписанный сертификат*, т.е. сам заверяет свой *ключ*.

В приведенном примере, CA_1 заверяет электронной подписью сертификаты подчиненных центров сертификации CA_2 и CA_3, а те, в свою *очередь*, подписывают *сертификаты пользователей* и центров более низкого уровня.

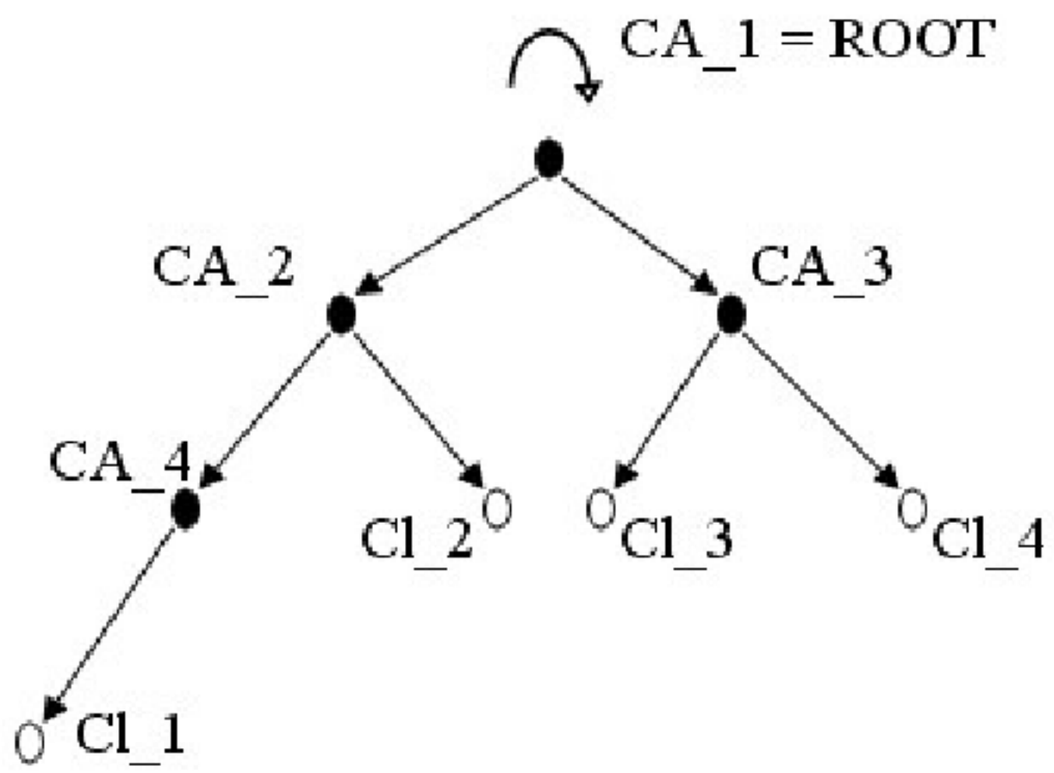

Рис. 3. Иерархия центров сертификации и клиентов

Перейдем к рассмотрению самих сертификатов. Наибольшее распространение получили цифровые сертификаты, формат которых определен стандартом X.509.

На данный момент, принята третья версия стандарта. Формат сертификата изображен на рис. 4.

Номер версии содержит числовое *значение*, соответствующее номеру версии (для сертификата версии 1 равен 0 и т.д.). В первой версии X.509 не было уникальных номеров ("*ID* Изготовителя", "*ID* Субъекта") и *полей расширения*. Во второй версии добавились указанные идентификаторы, в третьей - расширения.

Серийный номер - уникальный номер, присваиваемый каждому сертификату.

Алгоритм подписи - *идентификатор* алгоритма, используемого при подписании сертификата. Должен совпадать с полем **Алгоритм ЭЦП**.

Изготовитель - имя *центра сертификации*, выдавшего сертификат. Записывается в формате *Relative* Distinguished Name - RDN (варианты перевода названия - "относительное отдельное имя", "относительное характерное имя"). Данный формат используется в службах каталога, в частности, в протоколе *LDAP*.

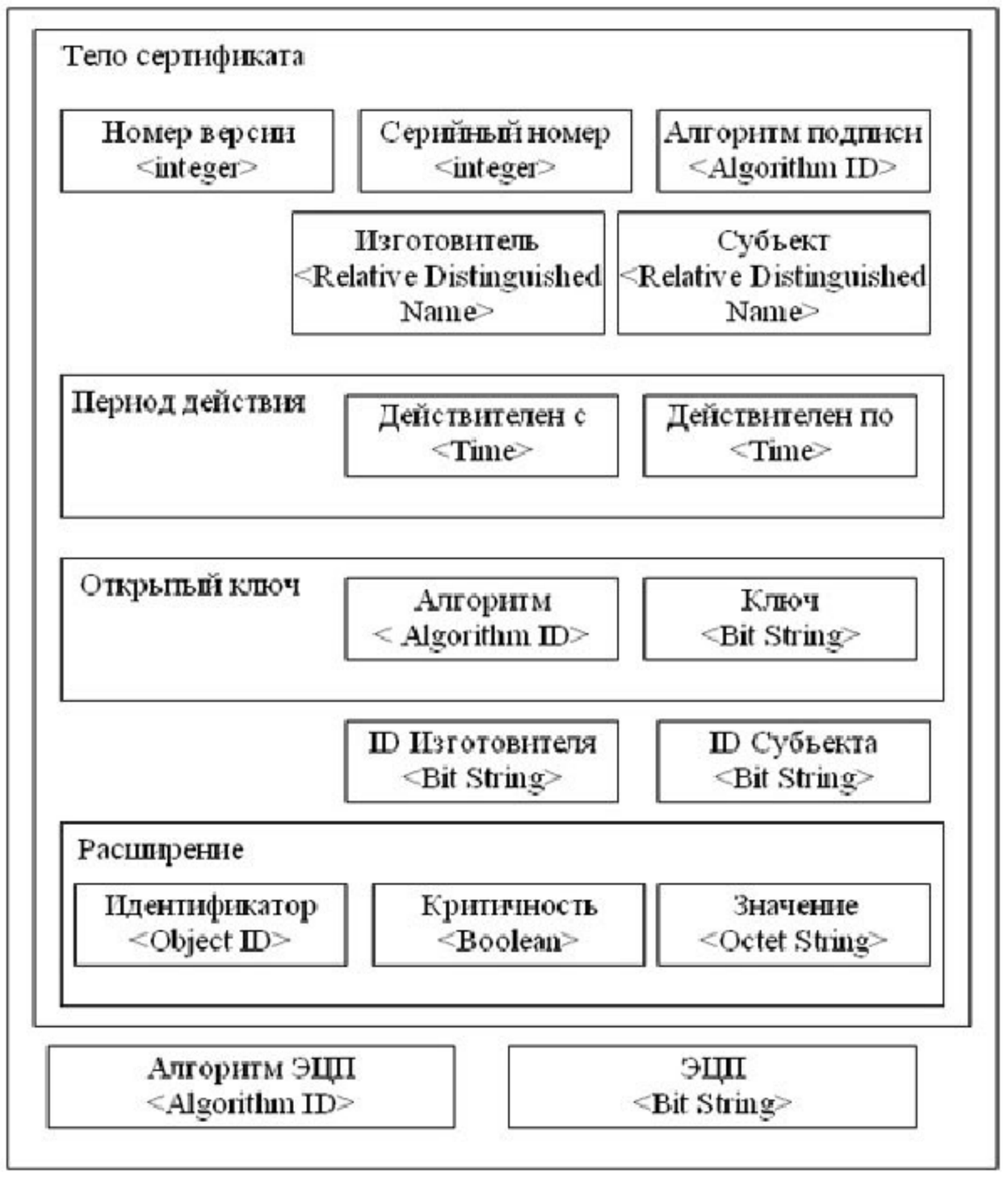

Рис. 4. Сертификат формата X.509 v.3

При записи *Relative* Distinguished Name используются специальные ключевые слова:

- CN (Common Name) - общее имя;
- OU (Organization Unit) - организационная единица;
- DC (Domain Component) - составная часть доменного имени.

Например, в сертификате Microsoft *Windows Hardware Compatibility*, который находится в *хранилище сертификатов Windows*XP *значение* данного поля следующее:

- CN = Microsoft Root Authority
- OU = Microsoft Corporation

- OU = Copyright (c) 1997 Microsoft Corp.

Как видно, указывается имя *центра сертификации*, компания, которой он принадлежит и т.д.

Субъект - имя владельца сертификата, представленное в том же формате RDN. Для указанного в предыдущем примере сертификата значения данного поля:

- CN = Microsoft Windows *Hardware Compatibility*
- OU = Microsoft Corporation
- OU = Microsoft Windows *Hardware Compatibility* Intermediate CA
- OU = Copyright (c) 1997 Microsoft Corp.

Период действия - описывает временной *интервал*, в течение которого *центр сертификации* гарантирует отслеживание *статуса сертификата*(сообщит абонентам сети о факте досрочного отзыва сертификата и т.д.). Период задается датами начала и окончания действия.

Открытый ключ - составное *поле*, содержащее *идентификатор* алгоритма, для которого предназначается данный открытый *ключ*, и собственно сам открытый *ключ* в виде набора битов.

ID Изготовителя и ID Субъекта содержат уникальные идентификаторы *центра сертификации* и пользователя (на случай совпадения имен различных *CA* или пользователей).

Расширения - дополнительный *атрибут*, связанный с субъектом, изготовителем или открытым ключом, и предназначенный для управления процессами сертификации. Более подробно он описан ниже.

Алгоритм электронной цифровой подписи (ЭЦП) - *идентификатор* алгоритма, используемый для подписи сертификата. Должен совпадать со значением поля **Алгоритм подписи**.

ЭЦП - само *значение* электронно-цифровой подписи для данного сертификата.

Расширения могут определять следующие дополнительные параметры:

- идентификатор пары открытый/секретный ключ *центра сертификации* (изготовителя), если центр имеет несколько различных ключей для подписи сертификатов;
- идентификатор конкретного ключа пользователя (субъекта), если пользователь имеет несколько сертификатов;
- назначение ключа, например, ключ для шифрования данных, *проверки ЭЦП* данных, для проверки *ЭЦП* сертификатов и т.д.;
- уточнение периода использования - можно сократить время действия сертификата, указанное в поле *Период действия* (т.е. период, в течение которого статус сертификата отслеживается, станет больше, чем разрешенное время использования сертификата);
- *политики использования* сертификата;
- выбор соответствия *политик использования* сертификата для *центра сертификации* и пользователя, если имеются различные варианты;
- *альтернативное имя* пользователя и *центра сертификации*;

• указания, является ли пользователь сам *центром сертификации* и насколько глубоко разрешается разворачивать *сертификационный путь*.

Предположим, что ключевые пары сгенерированы, открытые ключи заверены сертификатами и размещены в каталоге, реализованном с помощью *web-сервера*, ftp-сервера, службы каталога или другой технологии. Теперь, если *абонент* А желает проверить подпись абонента В под полученным сообщением (или зашифровать для В сообщение с помощью его открытого ключа и т.д.), он выполняет следующие действия:

1. запрашивает в сетевом справочнике сертификат C_B открытого ключа подписи (шифрования,...) абонента В;

2. проверяет достоверность сертификата C_B (см. ниже);

3. в случае успеха проверяет подпись под сообщением (зашифровывает сообщение,...) с помощью открытого ключа, извлеченного из C_B.

Процедура проверки достоверности сертификата C_B состоит в следующем:

1. проверяется срок действия сертификата C_B, если он закончился, сертификат считается недостоверным;

2. из C_B извлекается имя ЦС, подписавшего этот сертификат, обозначим его D ;

3. если D=B, то сертификат самоподписанный, он считается достоверным только, если D=ROOT (хотя, возможно, в некоторых сетях право выдавать самоподписанные сертификаты имеет не один ROOT, это - политика сети);

4. если же $D \neq B$, то из справочника запрашивается сертификат C_D открытого ключа подписи абонента D, проверяется на достоверность сертификат C_D;

5. в случае отрицательного ответа принимается решение о недостоверности сертификата C_B, иначе из C_D извлекается открытый ключ K_D;

6. с помощью K_D проверяется подпись под сертификатом C_B, по результатам проверки этой подписи судят о достоверности C_B.

Если ключи шифрования досрочно вышли из обращения (причины могут быть различны - *пользователь* увольняется из компании, *секретный ключ* скомпрометирован и т.д.), *центр сертификации* извещает об этом остальных пользователей сети путем выпуска списка отозванных сертификатов (англ. *Certificate* Revocation *List*, сокр. *CRL*). Структура *CRL* представлена на рис. 5.

Рис. 5. Структура списка отозванных сертификатов

Поля списка содержат следующую информацию:

- **Номер версии** определяет номер версии формата *CRL*. Текущая используемая версия - вторая.

- **Алгоритм подписи** - идентификатор алгоритма, с помощью которого подписан *CRL*. Должен совпадать по значению с полем **Алгоритм ЭЦП**.

- **Изготовитель** - имя *центра сертификации* в формате RDN.

- **Выпущен** - дата выпуска *CRL*.

- **Следующий** - дата, до которой будет выпущен следующий *CRL*.

- **Расширения** - описывают *центр сертификации*, точку для поиска *CRL* данного центра, номер данного списка и т.д.

- **Отозванный сертификат** - таких полей будет столько, сколько сертификатов отзывается - содержит номер отзываемого сертификата, дату, с которой сертификат отозван, описание причины отзыва.

- **Алгоритм ЭЦП** - идентификатор алгоритма *ЭЦП*, используемого для подписи списка.

- **ЭЦП** - сама *электронная цифровая подпись*.

Проблемы с *CRL* заключаются в том, что может возникнуть ситуация, когда *ключ* уже отозван, но *CRL* еще не выпущен, т.е. пользователи не могут получить информацию о компрометации ключа. Кроме того, распространение *CRL* идет *по* запросу клиента и нарушитель может препятствовать их получению.

Другая проблема *PKI* - *самоподписанные сертификаты*. Сертификат *ROOT* должен раздаваться всем абонентам сети в начале работы и сохраняться в защищенном от подделки хранилище. Иначе нарушитель может попробовать навязать свой сертификат в качестве сертификата корневого центра.

Мы рассмотрели случай реализации **иерархической модели** *PKI*, при которой *центры сертификации* организованы в древовидную структуру с корневым *центром сертификации* на верху иерархии. На практике также встречаются другие варианты организации:

- **одиночный центр сертификации**, который выдает себе *самоподписанный сертификат* - данная модель часто реализуется в небольших организациях, но она имеет отмеченный выше недостаток, связанный с *самоподписанными сертификатами*;

- **одноранговая модель**, при которой независимые *центры сертификации* взаимно сертифицируют друг друга.

Надо отметить, что сфера применения цифровых сертификатов сейчас достаточно широка. В частности, они используются для распределения открытых ключей в протоколах защиты электронной почты *S/MIME* или *PGP*, с помощью цифровых сертификатов проверяется подлинность участников соединения *по* протоколу *SSL* и т.д.

Начиная с *Windows 2000 Server* в состав *серверных ОС* Microsoft входит *программное обеспечение* для создания центров сертификации. Создание корпоративного ЦС может понадобиться, если принято решение использовать защиту электронной почты с помощью *S/MIME*, *шифрование данных* при хранении средствами *EFS* (*EFS* - Encrypted File *System* - реализует *шифрование данных* на дисках с файловой системой *NTFS*), *шифрование* сетевого трафика с помощью протокола IPSec.

Различные практические аспекты использования цифровых сертификатов рассматриваются в лабораторных работах № 6 и 7. Первая из них посвящена работе с сертификатами с точки зрения конечного пользователя (в том числе, получение сертификата для защиты электронной почты с помощью *S/MIME*), а вторая - созданию и администрированию *центра сертификации*. Вопросы использования *EFS* рассматриваются в работе № 8.

Контрольные вопросы:

1. Центры распределения ключей.
2. Инфраструктура открытых ключей.
3. Цифровые сертификаты.
4. Криптографический протокол.
5. Атака типа "человек посередине" (man in the middle).
6. Структура Key Infrastructure.
7. Иерархия центров сертификации и клиентов.
8. Сертификат формата X.509 v.3.
9. Структура списка отозванных сертификатов.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-3	1-2	1-3

Оценочные средства: собеседование.

3.8.ПРАКТИЧЕСКАЯ РАБОТА 8. Использование цифровых сертификатов.

Цель работы:

Получение и совершенствование практических навыков использования цифровых сертификатов.

Содержание:

Использование протоколов *SSL*/TSL. Центр сертификации VeriSign. Параметры сертификата. Защищенное хранилище ключей и сертификатов в операционной системе Windows. Подключение к системам Интернет-банкинга. Отозванные сертификаты к которым нет доверия. Выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Теоретический материал.

В ходе данной практической работы мы познакомимся с некоторыми вопросами использования цифровых сертификатов.

Начнем с их использования протоколом *SSL*/TSL (на самом деле это два разных протокола, но т.к. TSL разработан на базе *SSL*, принцип использования сертификатов один и тот же). 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. 8.1).

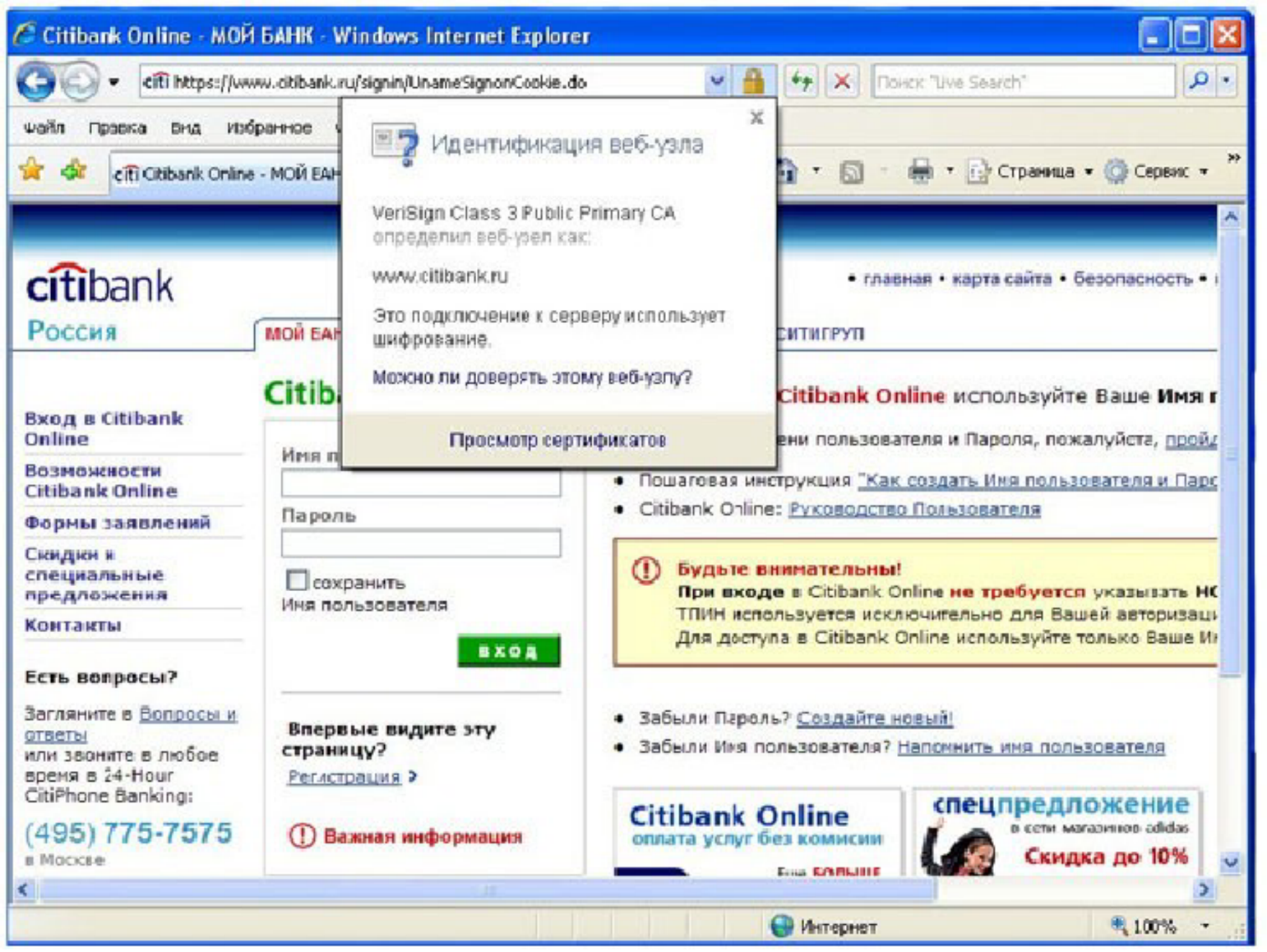

Рис. 8.1. Защищенное соединение

Префикс https в строке адреса и изображение закрытого замка справа от строки указывают, что установлено защищенное соединение. Если щелкнуть мышью *по* изображению замка, то увидим представленное на рис. 8.1 сообщение о том, что подлинность узла с помощью сертификата подтверждает *центр сертификации* VeriSign. Значит, мы на самом деле обратились на *сайт* Ситибанка (а не подделанный нарушителями *сайт*) и можем безопасно вводить логин и *пароль*.

Выбрав **"Просмотр сертификата"** можно узнать подробности о получателе и издателе, другие параметры сертификата (рис. 8.2).

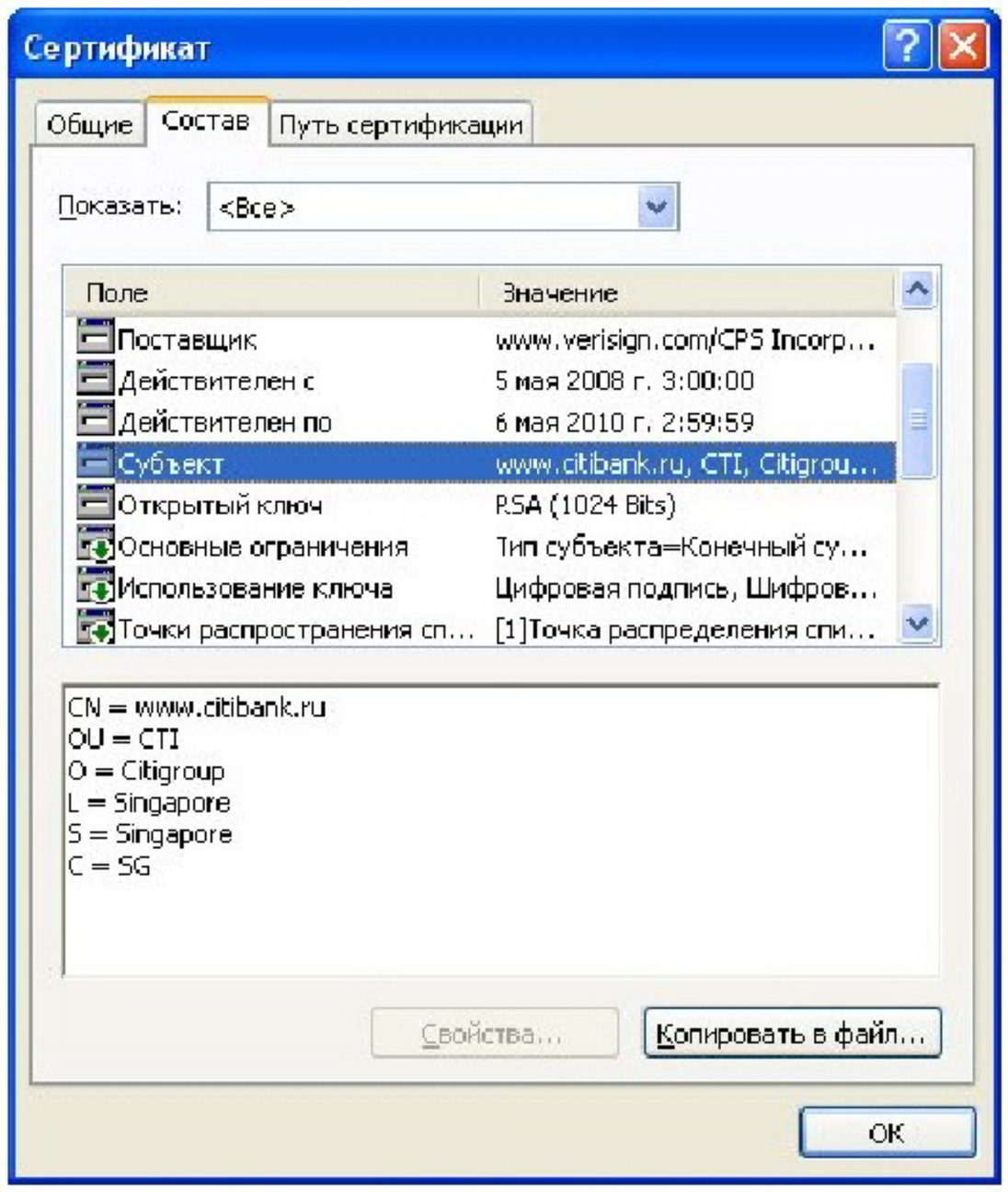

Рис. 8.2. Параметры сертификата

Задание

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

Теперь рассмотрим другой вариант - мы подключаемся *по SSL* 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. 8.3).

Если нажать ссылку **"Продолжить открытие этого web-узла"** можно будет просмотреть сертификат.

Задание

Разберитесь, в чем проблема с указанным сертификатом.

Примечание. На всякий случай в конце описания лабораторной приведен ответ.

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* ▯ **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.

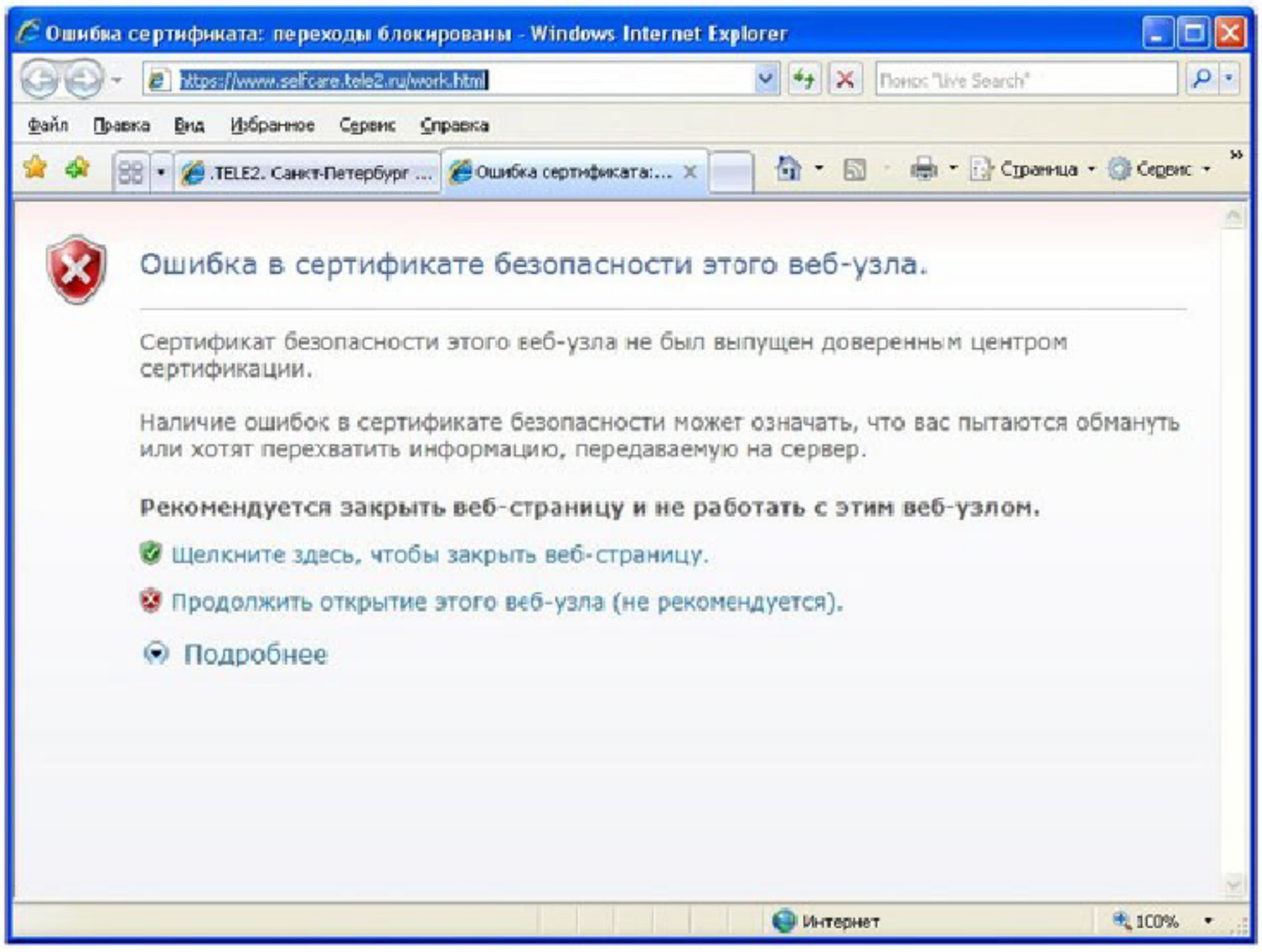

Рис. 6.3. Браузер сообщает о проблеме с сертификатом

Найдите в нем сертификат 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. 8.4).

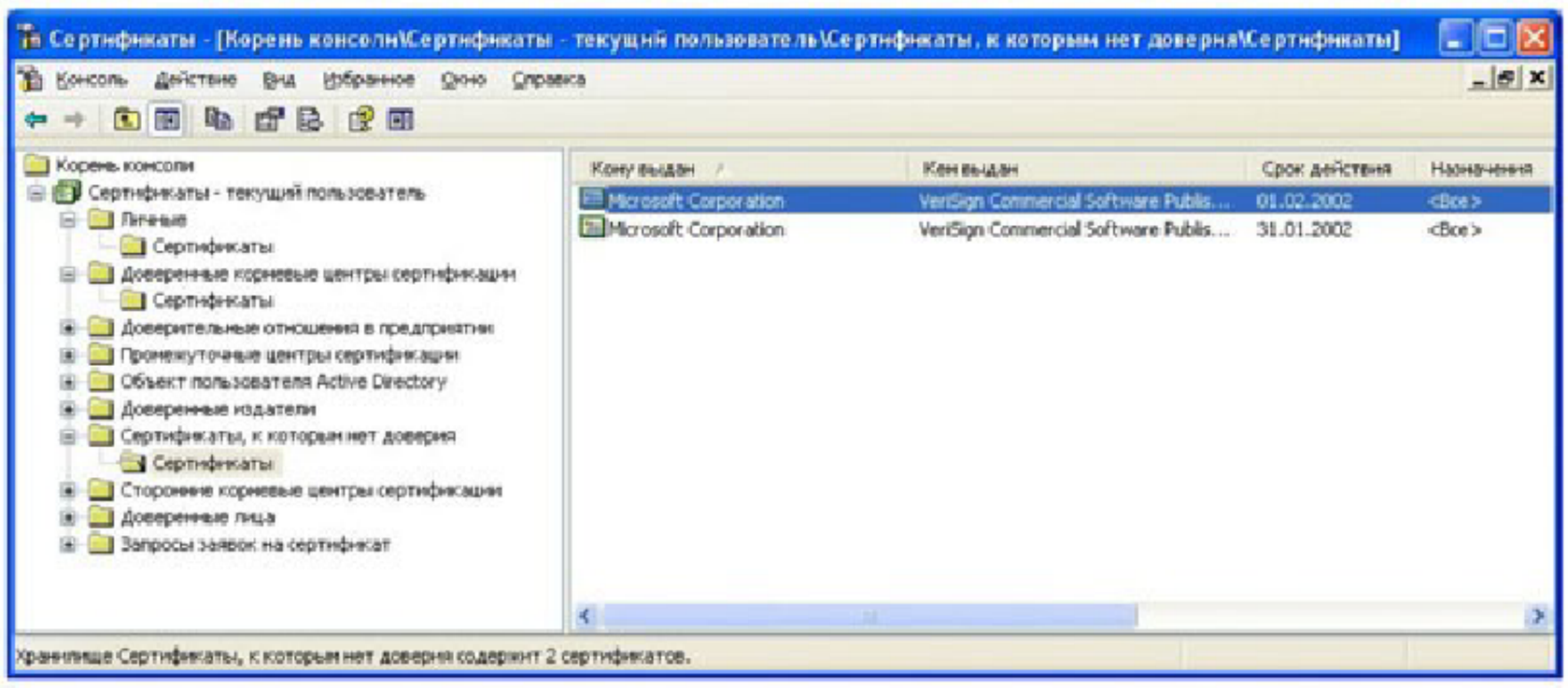

Рис. 8.4. Отозванные сертификаты

Теперь рассмотрим процесс запроса сертификата. На сайте *центра сертификации* Thawte http://www.thawte.com можно бесплатно получить сертификат для электронной почты. Для этого в *меню* сайта **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. 8.5).

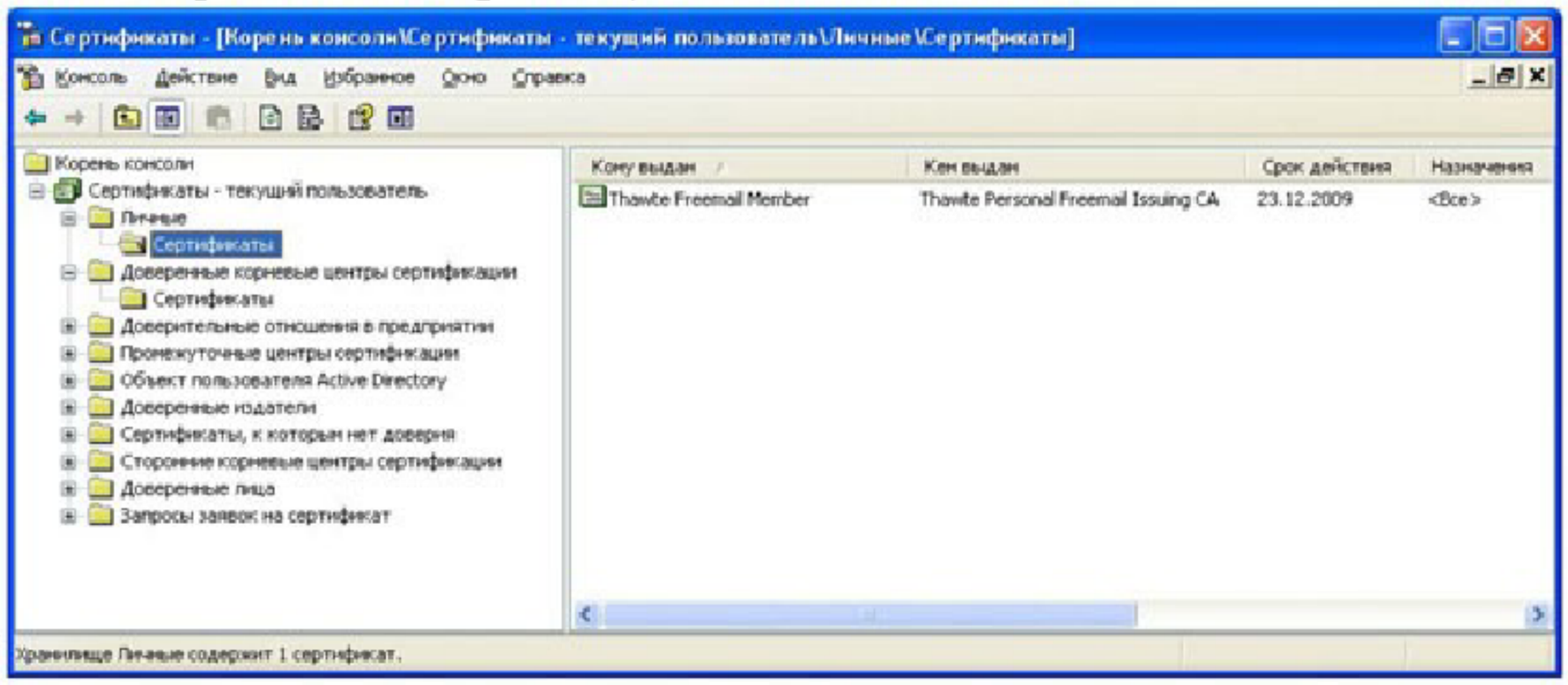

Рис. 8.5. Полученный сертификат

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. 8.6).

Задание

Запросите сертификат в Thawte и настройте *почтовый клиент* для использования *S/MIME*.

Проблема была в том, что сертификат "самоподписанный": он был выдан *центром сертификации* http://www.selfcare.tele2.ru самому себе. *Браузер* сообщает о невозможности удостовериться в подлинности узла из-за того, что данный *центр сертификации* отсутствует в списке доверенных, а проверить его подлинность с помощью "вышестоящего" по иерархии центра не представляется возможным (т.к. вышестоящего центра нет). Доверять или нет такому сертификату – каждый решает самостоятельно.

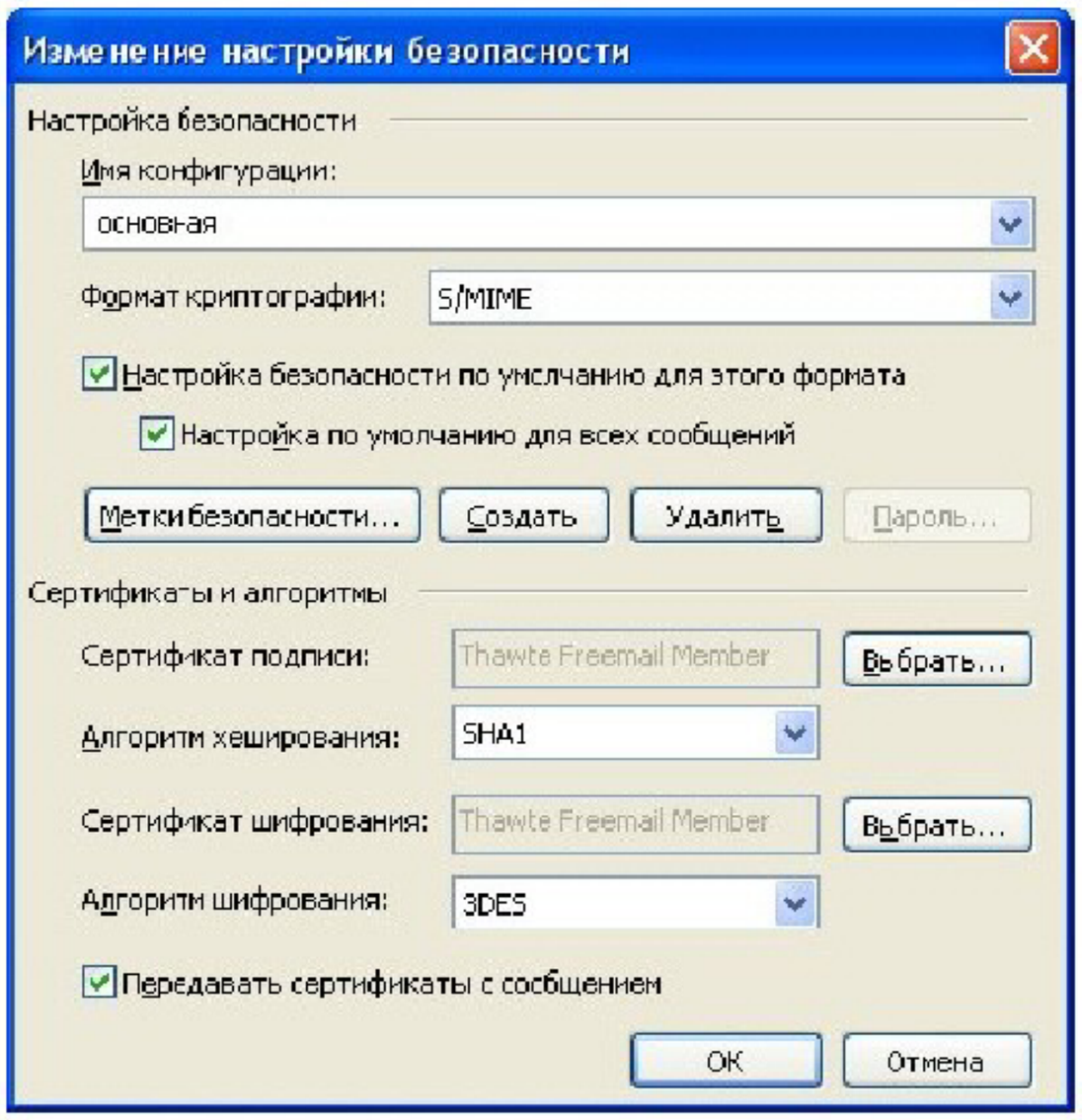

Рис. 8.6. Выбор сертификата для защиты почты с помощью S/MIME в Outlook

Контрольные вопросы:

1. Использование протоколов *SSL*/TSL.
2. Центр сертификации VeriSign.
3. Защищенное хранилище ключей и сертификатов в операционной системе Windows.
4. Подключение к системам Интернет-банкинга.
5. Отозванные сертификаты к которым нет доверия.
6. Выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-3	1-2	1-3

Оценочные средства: собеседование.

3.9.ПРАКТИЧЕСКАЯ РАБОТА 9. Резервное копирование в Windows Server 2008.

Цель работы:

Познакомиться со средствами организации резервного копирования в операционной системе Microsoft *Windows Server* 2008.

Содержание:

Утилиты администрирования. Полное резервное копирование и копирование отдельных дисков. Выбор дисков для резервного копирования. Доступные резервные копии для выбранного сервера. Выбор типа и параметров восстановления. Диск для хранения резервных копий. Выбор типа резервного копирования для диска.

Теоретическая часть

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. 9.1) и в появившемся списке выбрать *пункт* **Windows Server Backup Features** (рис. 9.2).

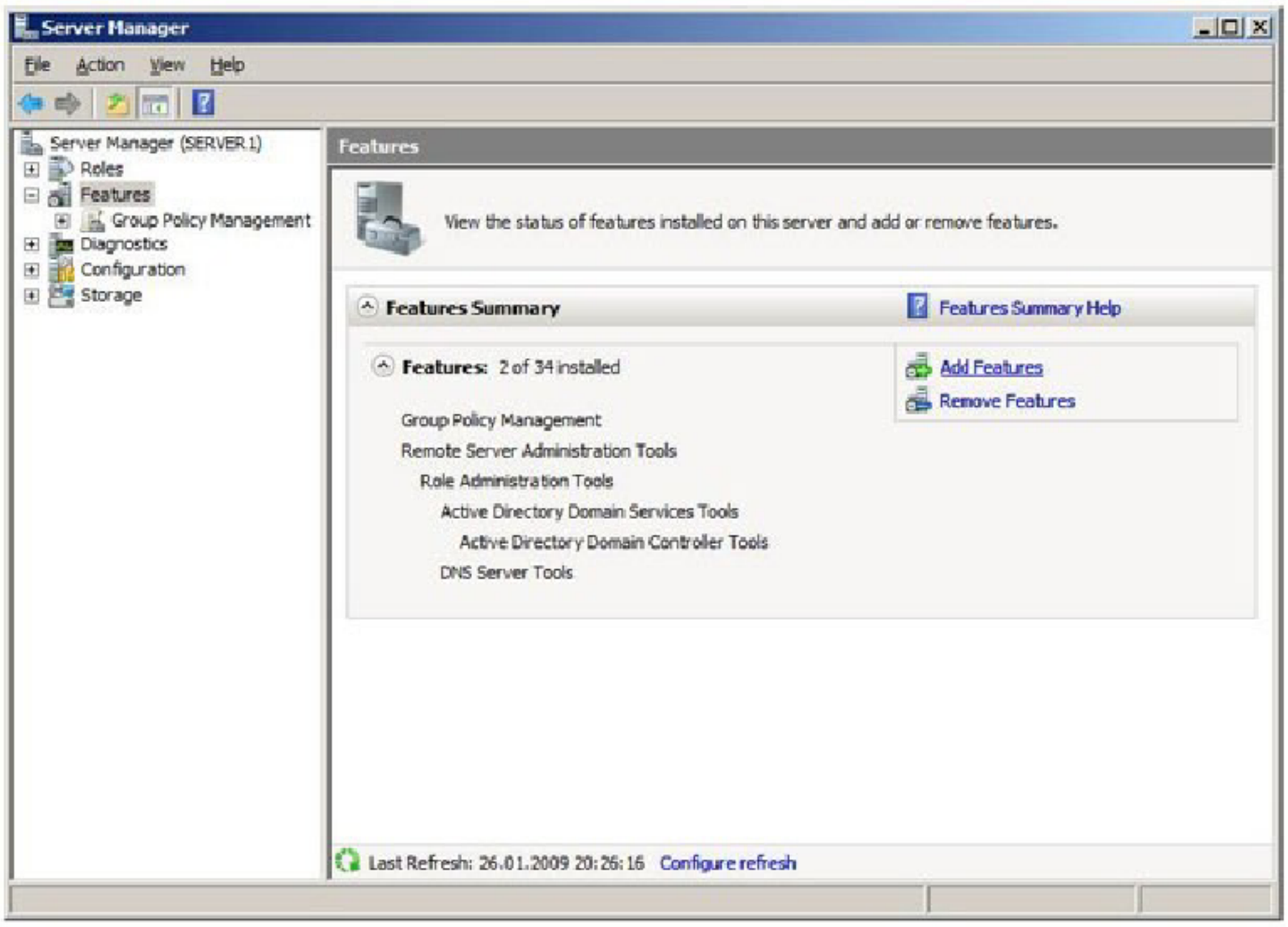

Рис. 9.1. Оснастка Server Manager позволяет добавить компоненты

Как видно на рис. 9.2, 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 Server Backup*.

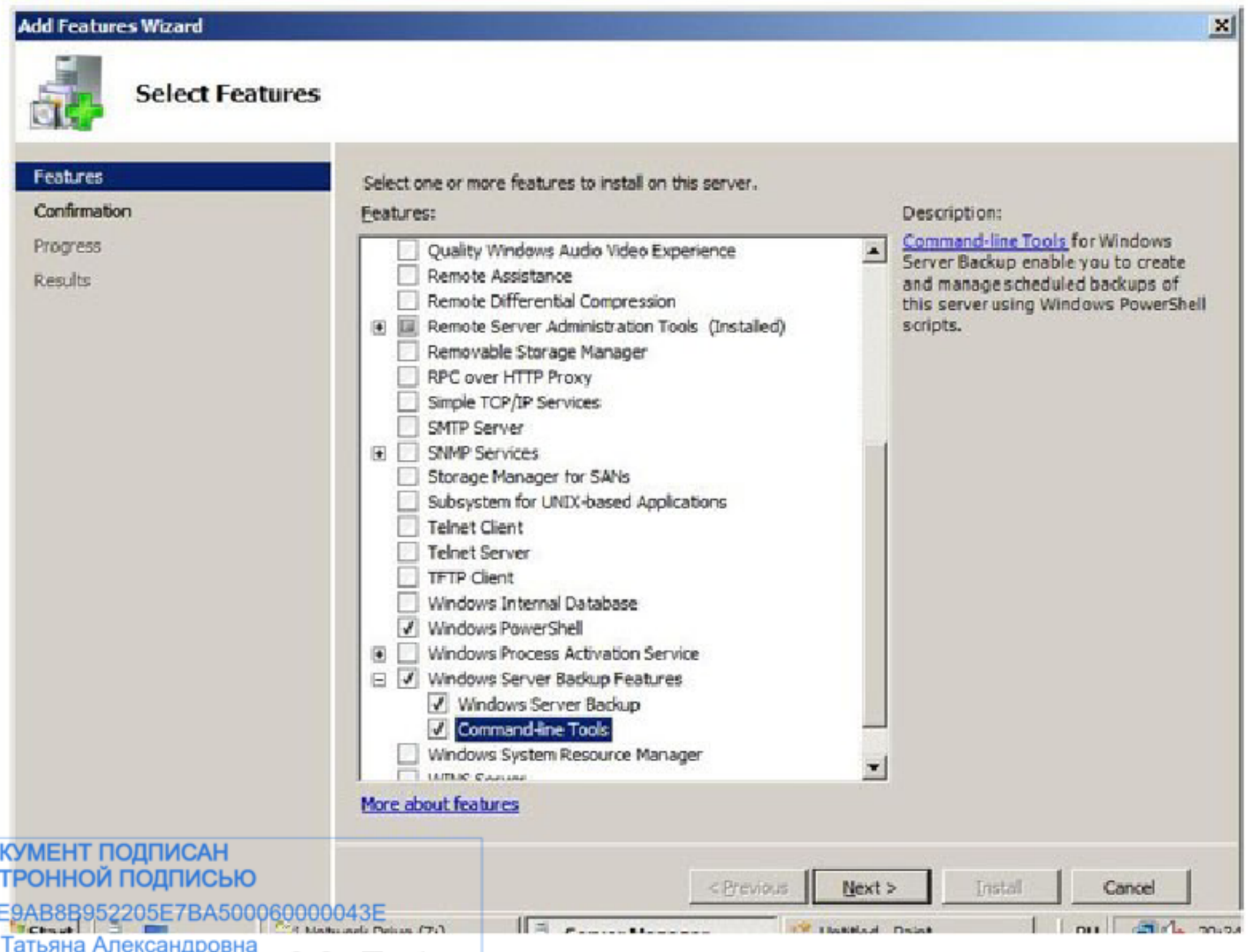

Рис. 9.2. Добавляем утилиты администрирования

После установки, в *меню* **Administrative Tools** становится доступной оснастка **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. 9.3). 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. 9.4). 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).

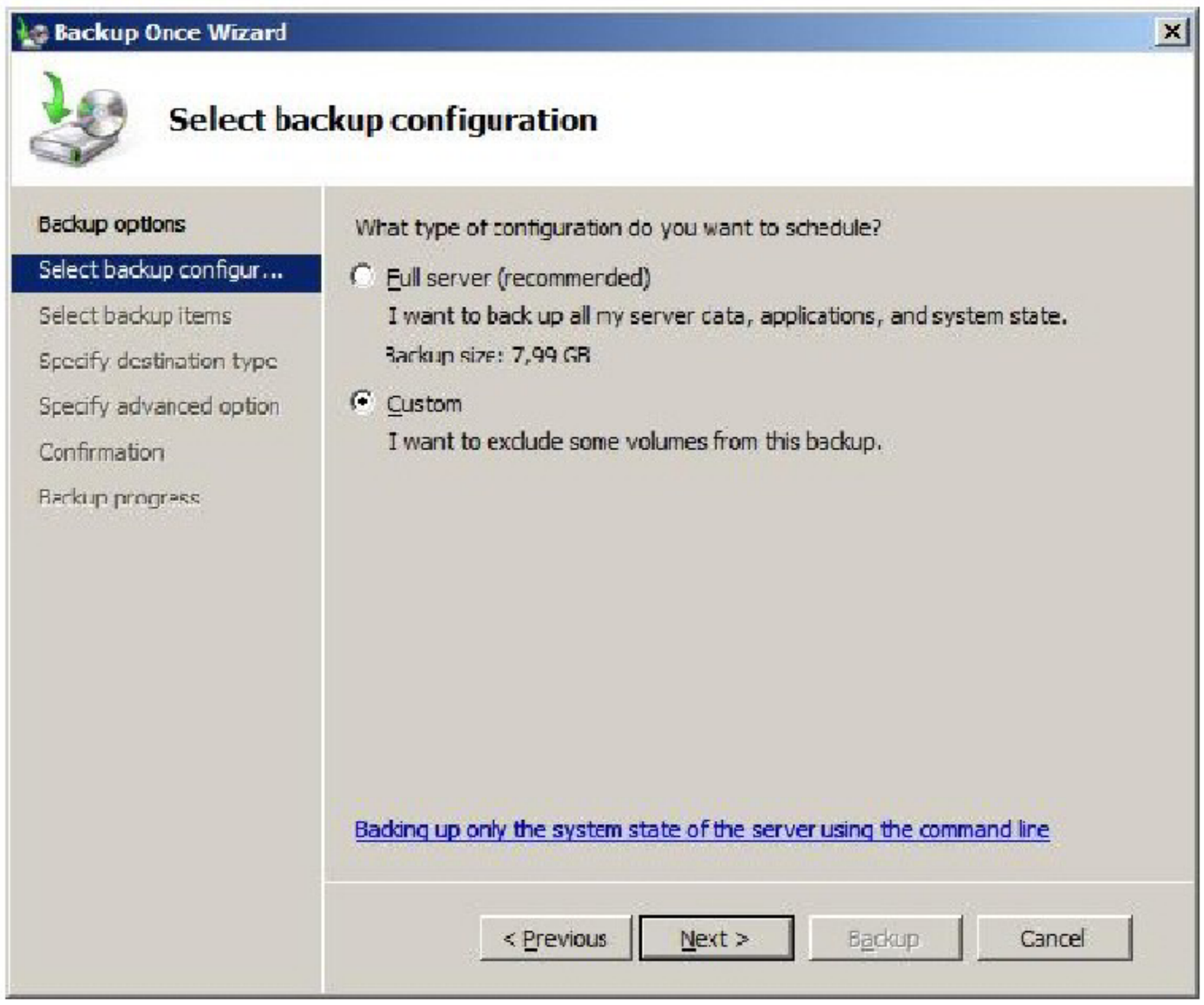

Рис. 9.3. Выбор между полным резервным копированием и копированием отдельных дисков

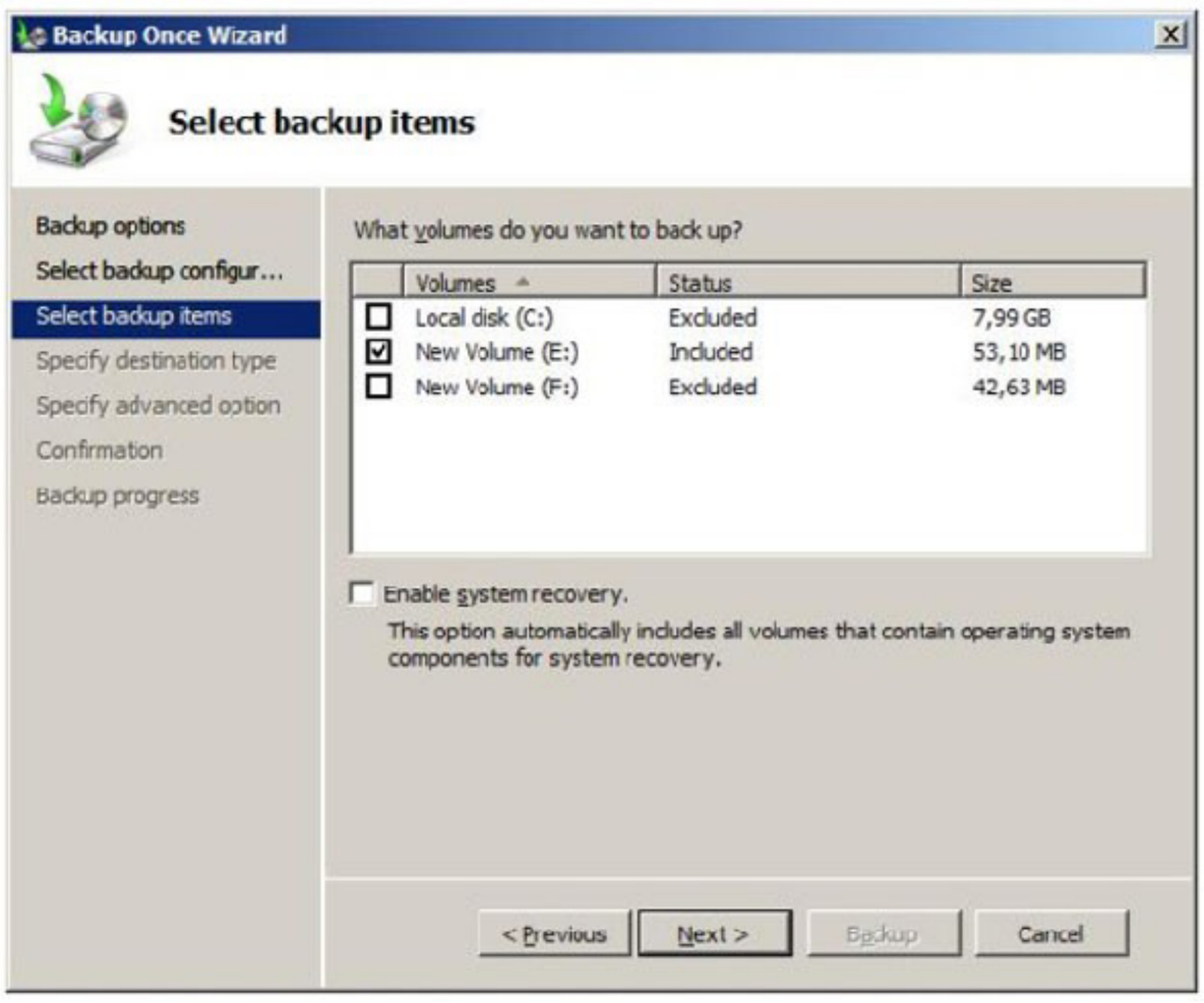

Рис. 10.4. Выбор дисков для резервного копирования

Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис. 9.4 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.

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. 9.5).

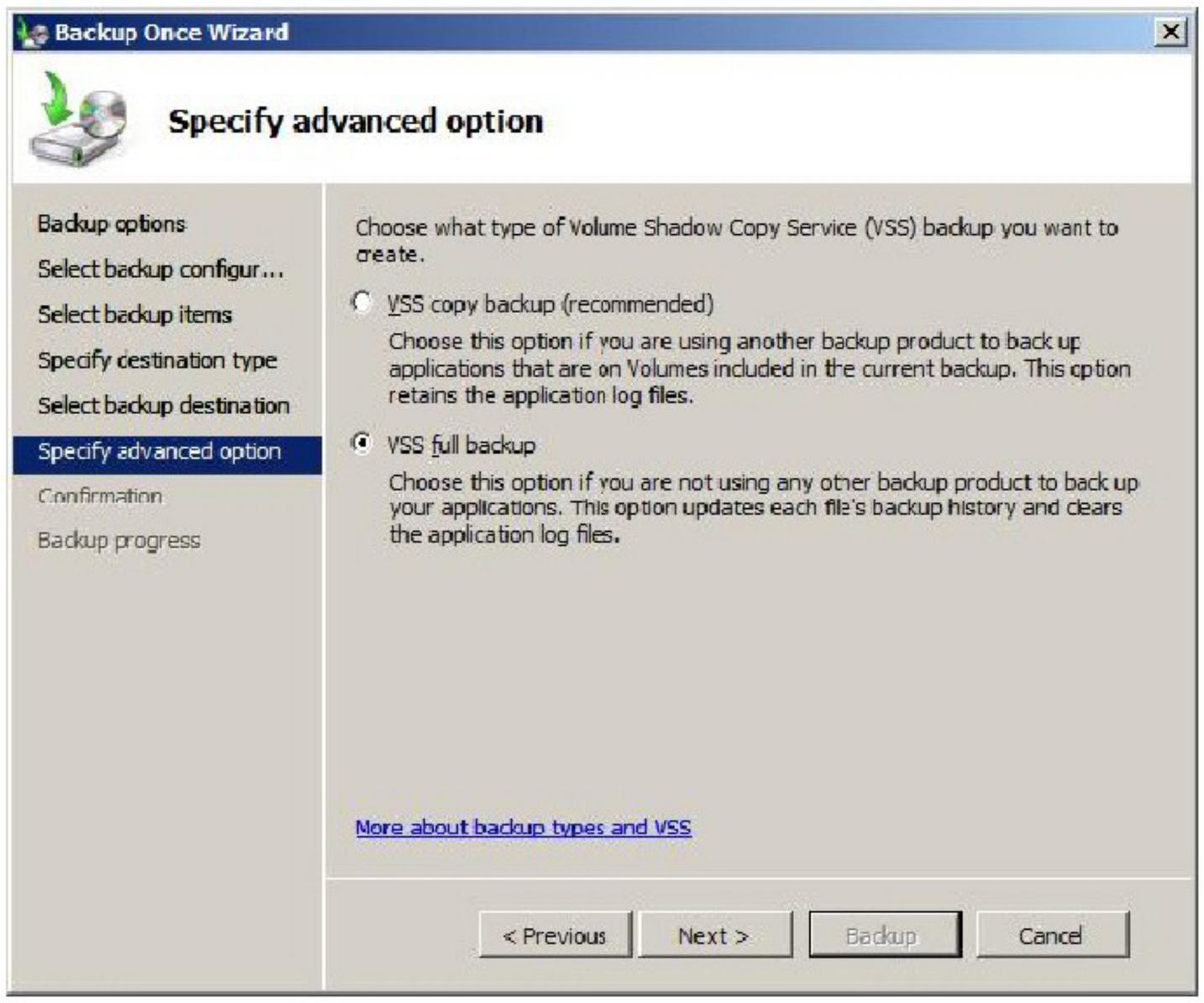

Рис. 9.5. Выбор типа копирования

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.

Задание

1. На учебном сервере (или виртуальной машине) выберите раздел для резервного копирования.

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

3. Выполните 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. 9.6).

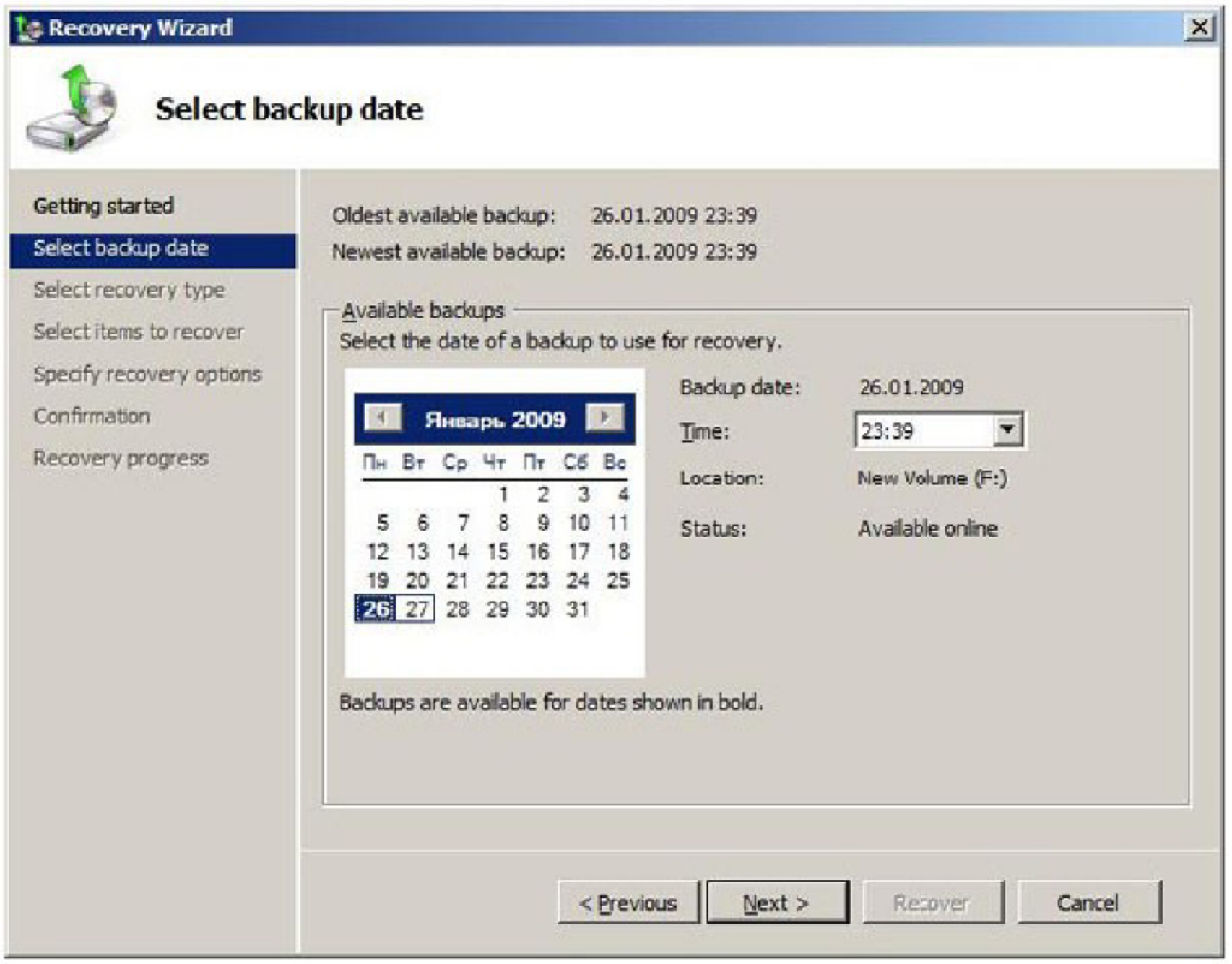

Рис. 9.6. Перечень доступных резервных копий для выбранного сервера

В следующем окне запрашивается, что именно восстанавливается. Нас интересует отдельная *папка*, потому выбираем вариант **Files and folders** (рис. 9.7). Другие варианты - восстановление зарегистрированных приложений и восстановление *раздела диска* целиком.

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. 9.8).

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.

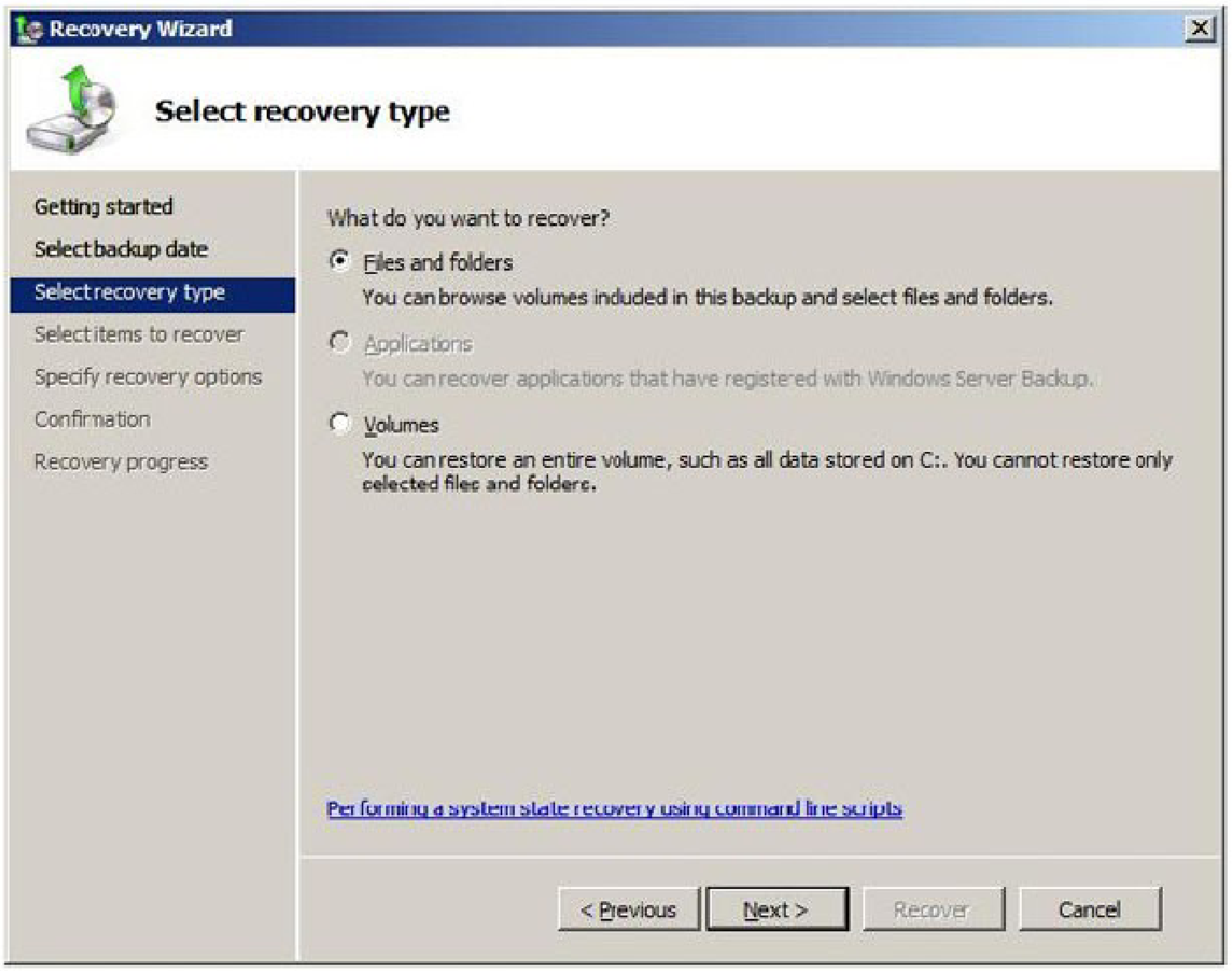

Рис. 9.7. Выбор типа восстановления

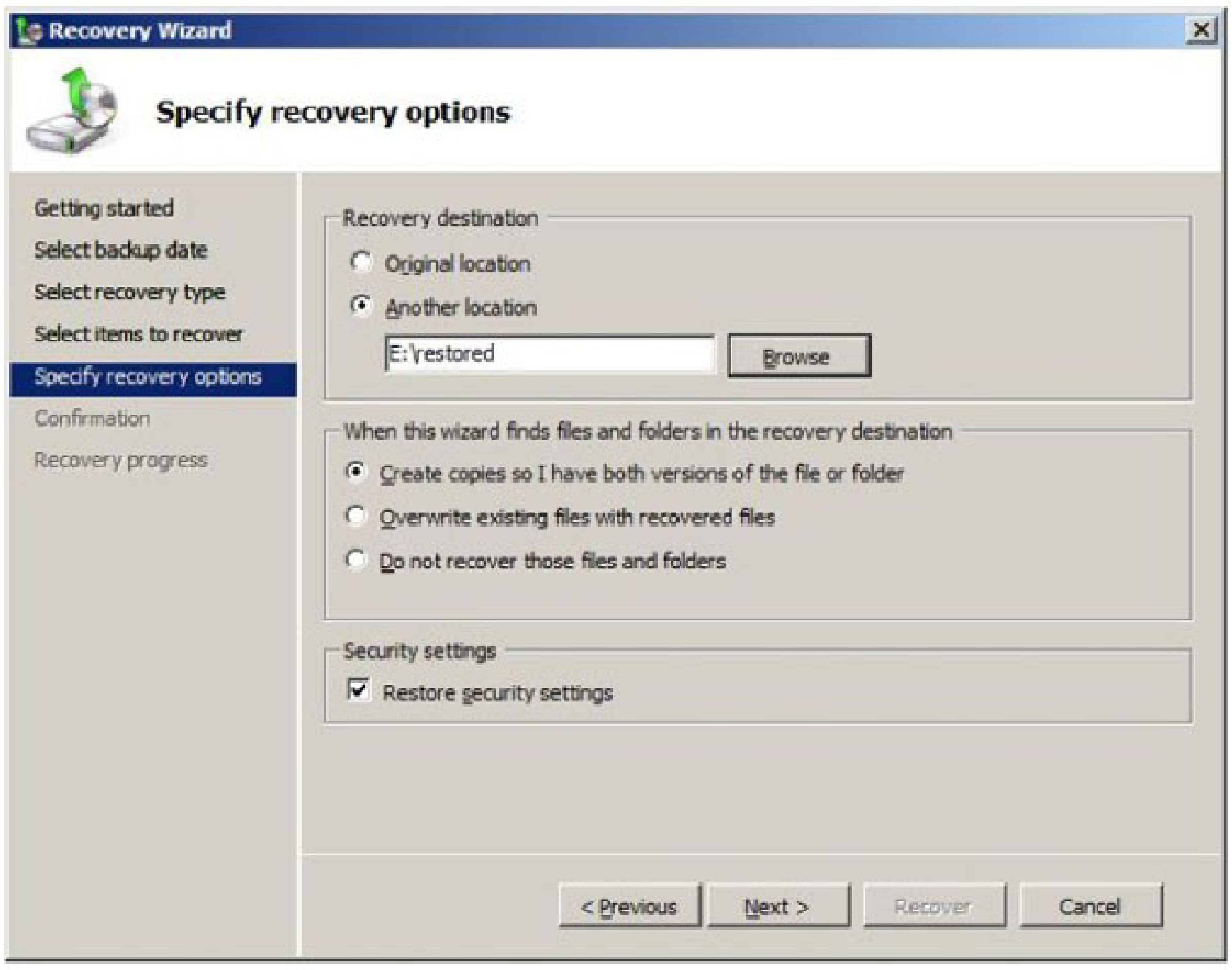

Рис. 9.8. Параметры восстановления

Задание

Выберите 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. Для этого в **Windows Server Backup** выберем опцию **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.

При этом надо учитывать:

1. даже при выборе резервного копирования отдельных разделов, в их список обязательно должен быть внесен раздел (-ы) с операционной системой;
2. копирование может выполняться один или несколько раз в день;
3. для хранения результатов резервного копирования должен выделяться отдельный диск, внутренний или внешний (например, подключаемый по USB). Перед началом использования, он будет отформатирован мастером архивации. Рекомендуется, чтобы он был не менее, чем в 1,5 раза больше по объему, чем архивируемые диски.

Пусть требуется ежедневно делать *резервное копирование* диска раздела с операционной системой. В окне мастера аналогичном рис. 9.3, выбираем вариант *Custom*, в окне аналогичном рис. 9.4 - *диск* C (на котором расположена *операционная система*). Указываем расписание (рис. 9.9).

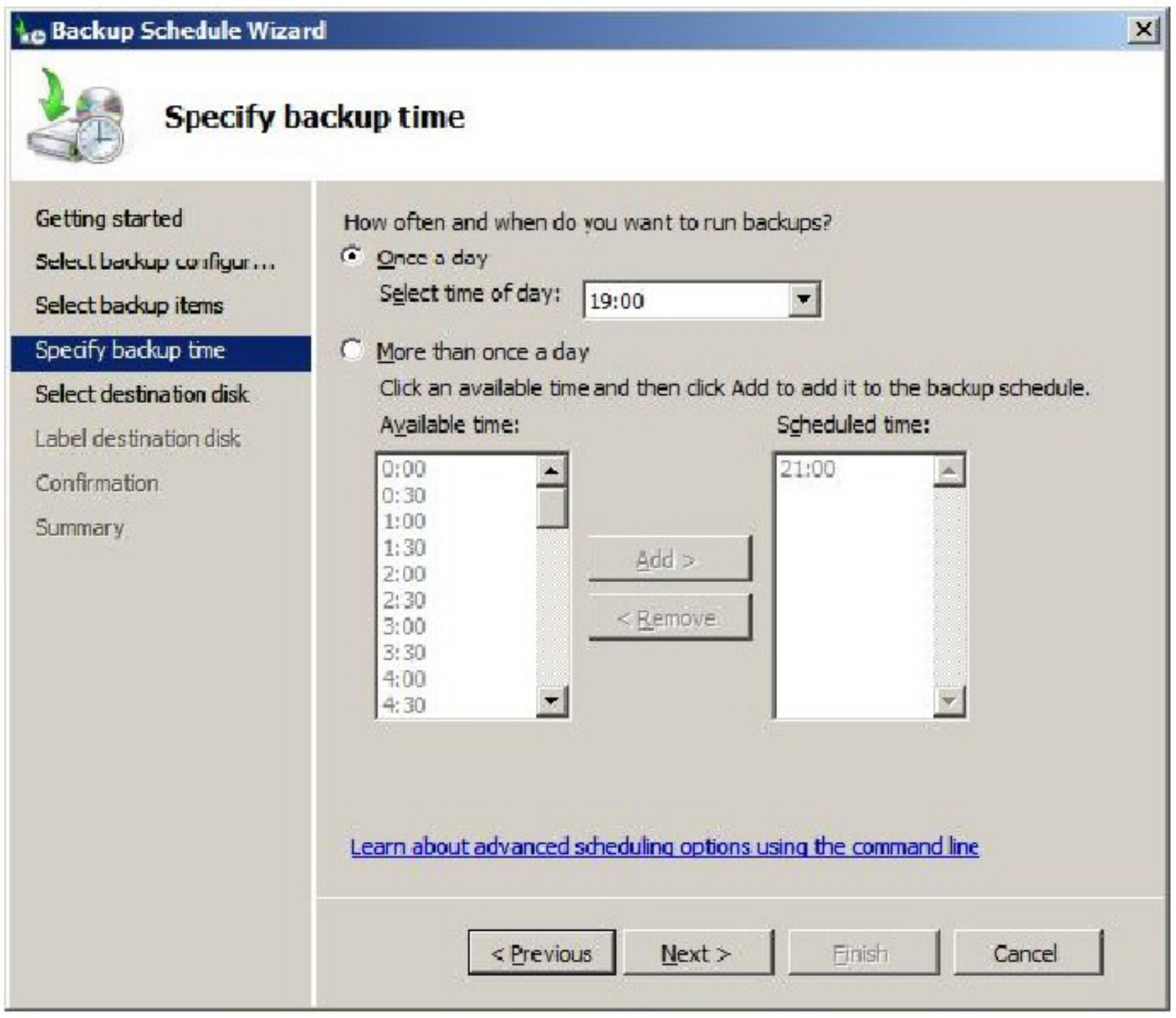

Рис. 9.9. Расписание резервного копирования

Дальше определяется *диск* (рис. 9.10), 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*.

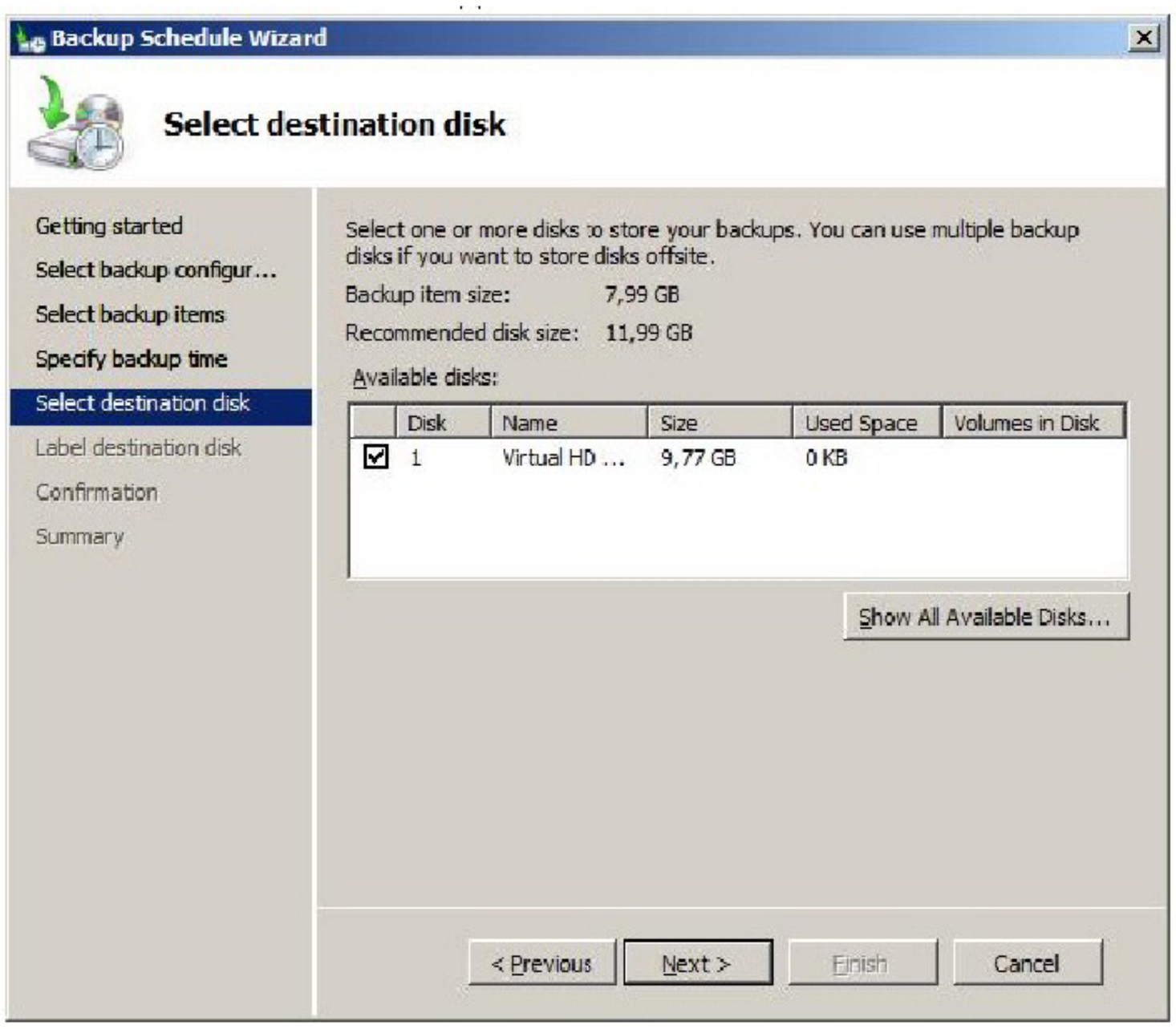

Рис. 9.10. Диск для хранения резервных копий

Когда работа *по* настройке автоматической архивации завершена, можно сделать дополнительные настройки, повышающие *быстродействие* для отдельных дисков. Для этого в списке **Actions** в оснастке **Windows Server Backup** выберите *пункт* **Configure Performance Settings**. В открывшемся окне (рис. 10.11) 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).

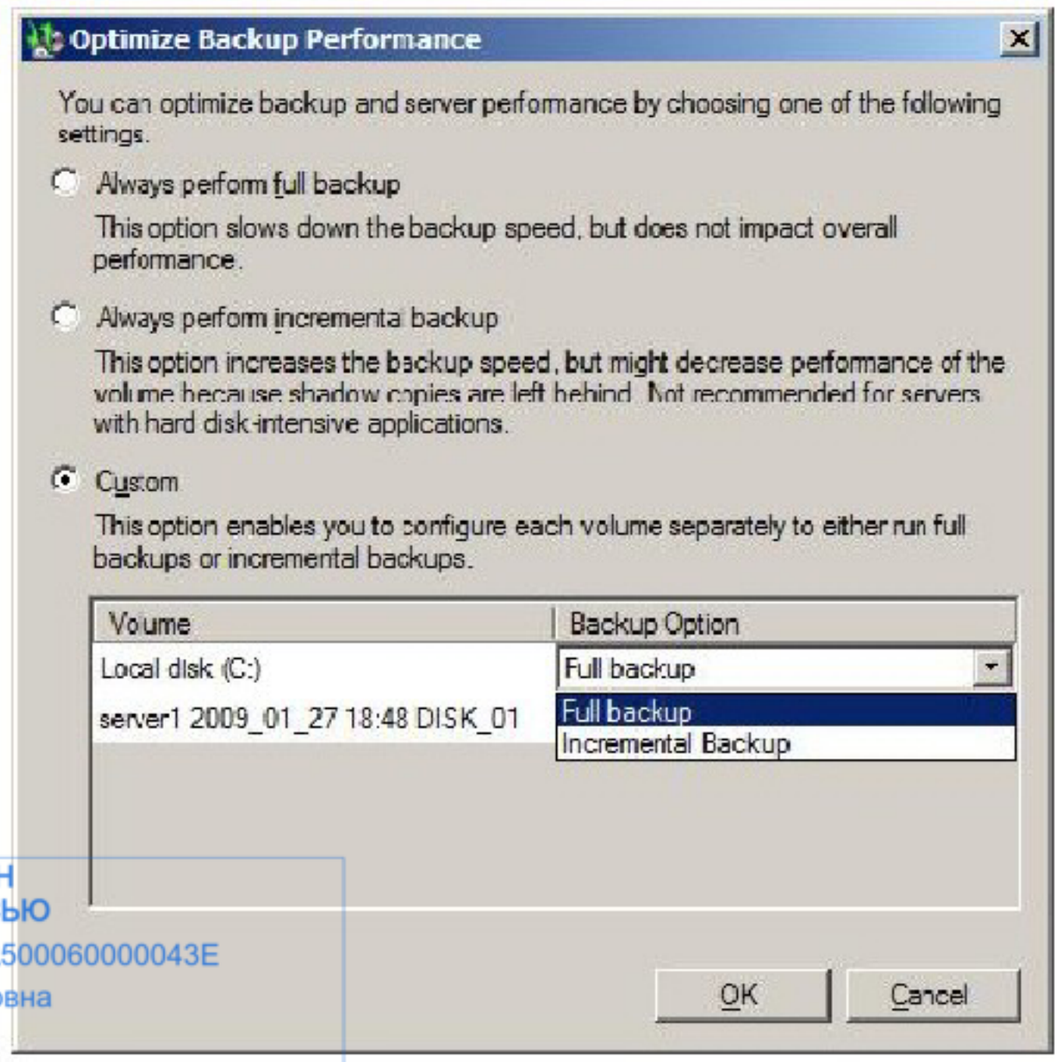

Рис. 9.11. Выбор типа резервного копирования для диска

Порядок восстановления такой же, как и при однократном копировании. Кстати, посмотреть параметры запланированного резервного копирования можно с помощью оснастки **Task Scheduler** (рис. 10.12).

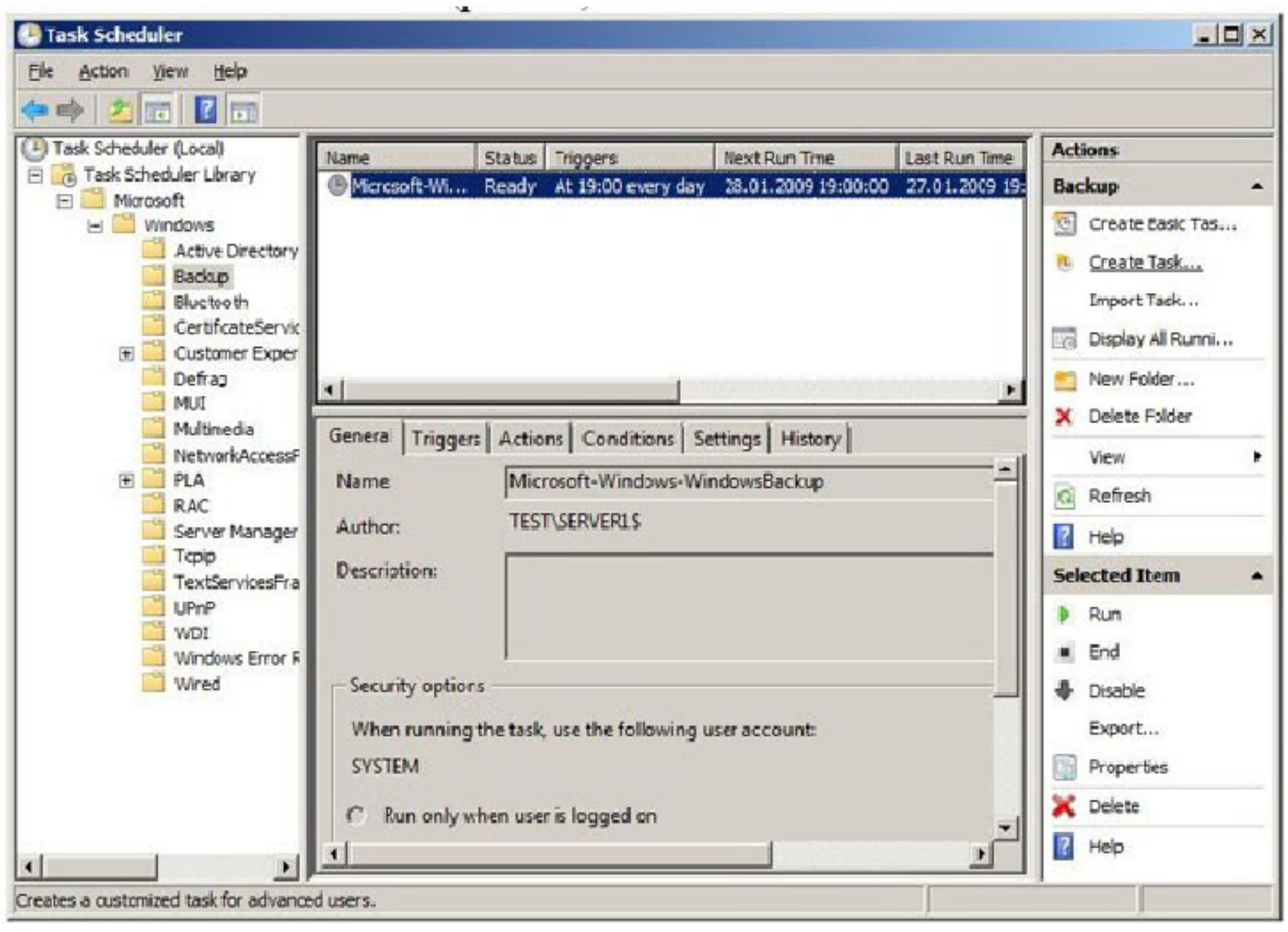

Рис. 9.12. Параметры созданного задания

Задание

Разработайте и реализуйте план ежедневного резервного копирования раздела с операционной системой.

При выполнении лабораторной работы на виртуальной машине для хранения резервных копий можно подключить дополнительный виртуальный *диск* (настройка делается в свойствах виртуальной машины, когда она не запущена). При выполнении работы на учебном севере, заранее определите физический *диск*, на который можно сохранить копии (*диск* не должен содержать полезных данных, т.к. он будет отформатирован!).

Выберите такое время создания копии, чтобы результат можно было увидеть в ходе выполнения лабораторной.

После создания копии, восстановите какой-либо из файлов.

Используя опцию **Backup Schedule** оснастки **Windows Server Backup**, удалите запланированное задание на *резервное копирование*.

Контрольные вопросы:

1. Утилиты администрирования.
2. Выбор дисков для резервного копирования.
3. Доступные резервные копии для выбранного сервера.
4. Выбор типа и параметров восстановления.
5. Диск для хранения резервных копий.
6. Выбор типа резервного копирования для диска.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-3	1-2	1-3

Оценочные средства: собеседование.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

3.1. Рекомендуемая литература

3.1.1. Основная литература:

1. Царев, Р.Ю. Программные и аппаратные средства информатики: учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

3.1.2. Дополнительная литература:

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

1.3. Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Программно-аппаратные средства защиты информации».
2. Методические указания по выполнению практических работ по дисциплине «Программно-аппаратные средства защиты информации».
3. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Программно-аппаратные средства защиты информации»

3.1.4. Интернет-ресурсы:

http://www.biblioclub.ru/ - электронная библиотека
http://www.uts-edu.ru/ - «Электронные курсы»

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы по дисциплине «ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2023

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Программно-аппаратные средства защиты информации» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-6	Способен при решении профессиональной задач организовывать защиту информации по ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федерации службы по техническому и экспортному контролю.
ОПК-1.4	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
5 семестр					
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Самостоятельное изучение литературы и источников	Собеседование	6,075	0,675	6,75
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к лабораторным занятиям	Отчет письменный	6,075	0,675	6,75
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к практическим занятиям	Отчет письменный	6,075	0,675	6,75
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к лекциям	Собеседование	6,075	0,675	6,75
Итого за 5 семестр			24,3	2,7	27
6 семестр					
ОПК-6	Самостоятельное	Собеседован	19,98	2,22	22,2

(ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	изучение литературы и источников	ие			
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к лабораторным занятиям	Отчет письменный	6,48	0,72	7,2
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к практическим занятиям	Отчет письменный	2,16	0,24	2,4
ОПК-6 (ИД-1 ИД-2 ИД-3) ОПК-1.4 (ИД-1 ИД-2 ИД-3)	Подготовка к лекциям	Собеседование	1,08	0,12	1,2
Итого за 6 семестр			29,7	3,3	33
Итого			54	6	60

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;

● шрифт Times New Roman;

● кегль шрифта 14;

● межстрочное расстояние 1,5;

● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;

● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на

основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласовать с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен,	Технические средства и информационные технологии освоены и использованы для реализации	Студент проявил инициативу, творческий подход, способность к выполнению сложных	Проект представлен полностью и в срок.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	проекта полностью	заданий, навыки работы в коллективе, организационные способности.	
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Царев, Р.Ю. Программные и аппаратные средства информатики: учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 160 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-7638-3187-0 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=435670

2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс] / . — Электрон. Текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 31 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

Дополнительная литература:

1. Айдинян, А.Р. Аппаратные средства вычислительной техники : учебник / А.Р. Айдинян. - М. ; Берлин : Директ-Медиа, 2016. - 125 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-4475-8443-6 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=443412

2. Привалов, И. М. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Основы аппаратного и программного обеспечения : учеб.-метод. пособие / И.М. Привалов ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 145 с. - 144 с.

Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Программно-аппаратные средства защиты информации».

2. Методические указания по выполнению практических работ по дисциплине «Программно-аппаратные средства защиты информации».

3. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Программно-аппаратные средства защиты информации»

Интернет-ресурсы:

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»