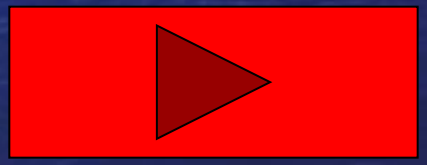
Практическое занятие № 6. Работа с шифрующей файловой системой на примере EFS

Цель: Научиться использовать EFS и программную утилиту cipher для реализации криптографической защиты данных.

Начать показ слайдов



По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

Теоретическая часть

Самая серьезная и, к сожалению, нередко встречающаяся ошибка при работе с EFS заключается в том, что пользователи шифруют данные на локальном компьютере (или компьютере — члене группы), а затем переустанавливают операционную систему. В этом случае *данные будут безвозвратно утеряны*, т. к. доступ к ним имели только два пользователя той системы, в которой данные были зашифрованы: пользователь, выполнивший эту операцию, и *агент восстановления*. Ошибка состоит в том, что для расшифровки данных необходимо предъявить сертификаты одного из названных пользователей, а для этого эти сертификаты нужно было экспортировать и сохранить.

По умолчанию на изолированных компьютерах под управлением Windows XP агенты восстановления не создаются и политика восстановления не определена. Это означает, что восстановить зашифрованную информацию могут только те пользователи, которые ее зашифровали. В домене всегда имеется агент восстановления — по умолчанию им является пользователь Администратор (Administrator) и определена политика восстановления.

EFS располагает встроенными средствами восстановления зашифрованных данных в условиях, когда неизвестен личный ключ пользователя. Необходимость подобной операции может возникнуть в следующих случаях:

- **Пользователь был уволен из компании и ушел, не сообщив свой пароль. Работа с зашифрованными файлами такого пользователя невозможна.**
- **Пользователь утратил свой личный ключ.**
- **Органы государственной безопасности направили запрос на получение доступа к зашифрованным данным пользователя.**

Windows XP позволяет создать необходимые ключи для восстановления зашифрованных данных в описанных ситуациях. Пользователи, которые могут восстанавливать зашифрованные данные в условиях утраты личного ключа, называются *агентами восстановления данных.* Агенты восстановления данных обладают сертификатом (X509 version 3) на восстановление файлов и личным ключом, с помощью которых выполняется операция восстановления зашифрованных файлов. Используя ключ восстановления, можно получить только сгенерированный случайным образом ключ, с помощью которого был зашифрован конкретный файл. Поэтому агенту восстановления не может случайно стать доступной другая конфиденциальная информация.

Средство восстановления данных предназначено для применения в разнообразных конфигурациях вычислительных сред. Параметры процедуры восстановления зашифрованных данных в условиях утраты личного ключа задаются *политикой восстановления.* Она представляет собой одну из политик открытого ключа. Политика восстановления автоматически создается только на контроллерах домена. Администратор домена одновременно является и агентом восстановления с соответствующими полномочиями. Могут быть добавлены и другие агенты.

Для создания *агента восстановления домена* необходимо:

1. Запустить оснастку *Групповая политика (Group Policy).*

2. Раскрыть узел *Конфигурация компьютера* | *Конфигурация Windows* | *Параметры безопасности* | *Политики открытого ключа* | *Файловая система EFS (Computer Settings* | *Security Settings* | *Public Key Policies* | *Encrypting File System).*

3. Выполнить в контекстном меню команду *Добавить (Add)* или *Создать (Create)* (в первом случае выбирается пользователь с *имеющимся* сертификатом агента восстановления, во втором — запрашивается и устанавливается *новый* сертификат для текущей учетной записи).

Политика восстановления может быть задана и на одиночном компьютере.

Из вышесказанного следует, что политика восстановления определяется только для *компьютера,* но не для *пользователя.*

Создание агента восстановления

Описываемая ниже процедура должна выполняться на автономном компьютере, на котором планируется использование системы EFS. Сначала необходимо создать сертификат агента восстановления (лучше использовать административную учетную запись, хотя, строго говоря, это не обязательно), импортировать его, а затем назначить политику восстановления.

Чтобы создать сертификат агента восстановления:

1. **Войдите в систему как администратор.**

2. **В окне консоли введите команду *cipher /R:имяФайла* — без расширения.**

3. **Введите и подтвердите пароль, защищающий личный ключ.**

В текущем каталоге будут созданы два файла: с расширением *cer* (содержит только сгенерированный ключ) и с расширением *pfx* (содержит и ключ, и сертификат агента восстановления). Для большей сохранности перепишите файлы на дискету.

Для импорта сертификата, с помощью которого можно восстанавливать индивидуальные файлы пользователей:

1. **Зарегистрируйтесь в системе как администратор.**

2. **Запустите оснастку *Сертификаты (Certificates)*, откройте узел *Личные (Personal)*, а затем папку *Сертификаты*.**

3. **Импортируйте созданный PFX-файл. (Подробно импорт сертификатов описан ниже.)**

Чтобы определить политику агента восстановления для любых операций шифрования:

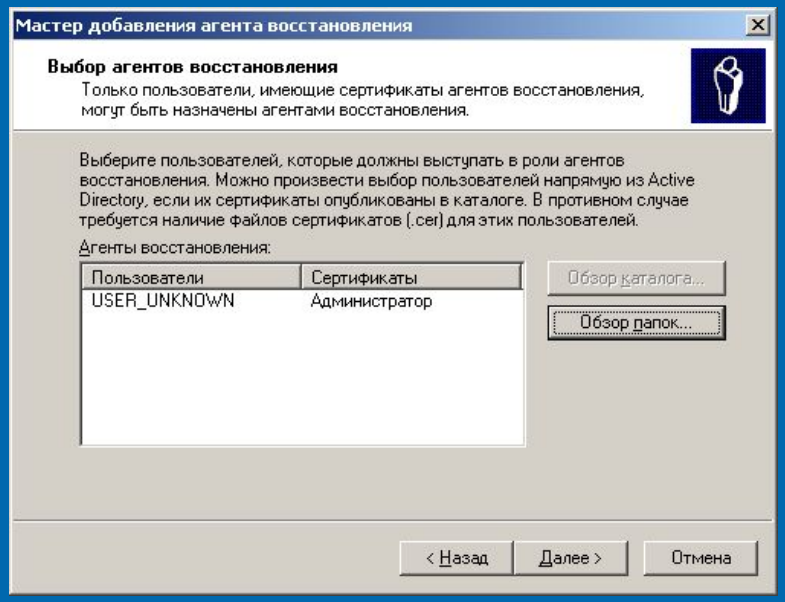
1. Запустите оснастку *Локальные параметры безопасности* (*Local Security Settings*).

2. Выберите узел *Политики открытого ключа* | *Файловая система EFS (Public Key Policies* | *Encrypting File System).*

3. В контекстном меню выполните команду *Добавить агента восстановления данных (Add Data Recovery Agent).*

4. В окне *Мастера добавления агента восстановления* (*Add Recovery Agent Wizard*) нажмите кнопку *Обзор папок (Browse Folders)* и выберите местоположение созданного ранее файла сертификата с расширением *cer*.

5. Пример окна мастера, содержащего сертификат, пригодный для импорта, показан на рисунке. (Имя пользователя неизвестно, поскольку оно не хранится в файле — это нормальная ситуация.)



6. Нажмите кнопку *Далее (Next)* и в следующем окне мастера — *Готово (Finish)*.

Сертификат будет импортирован и его владелец станет агентом восстановления на данном компьютере. Обратите внимание на то, что в столбце *Назначение (Intended Purposes)* импортированного сертификата указано *Восстановление файлов (File Recovery)*. Теперь можно использовать шифрование информации, не опасаясь потери "ключа" к ней.

Шифрование файлов и каталогов

Поскольку шифрование и дешифрование выполняется автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Например, можно так же открыть текстовый процессор Word, загрузить документ и отредактировать его, как и прежде. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Следует отметить, что пользователи (в данном случае администраторы) не должны шифровать файлы, находящиеся в системном каталоге, поскольку они необходимы для загрузки системы, в процессе которой ключи пользователя недоступны. Это сделает невозможным дешифрование загрузочных файлов, и система потеряет работоспособность. Проводник предотвращает возможность возникновения такой ситуации, не позволяя шифровать файлы с атрибутом *системный*.

Шифрование информации задается в окне свойств файла или папки:

1. **Укажите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду *Свойства (Properties).***

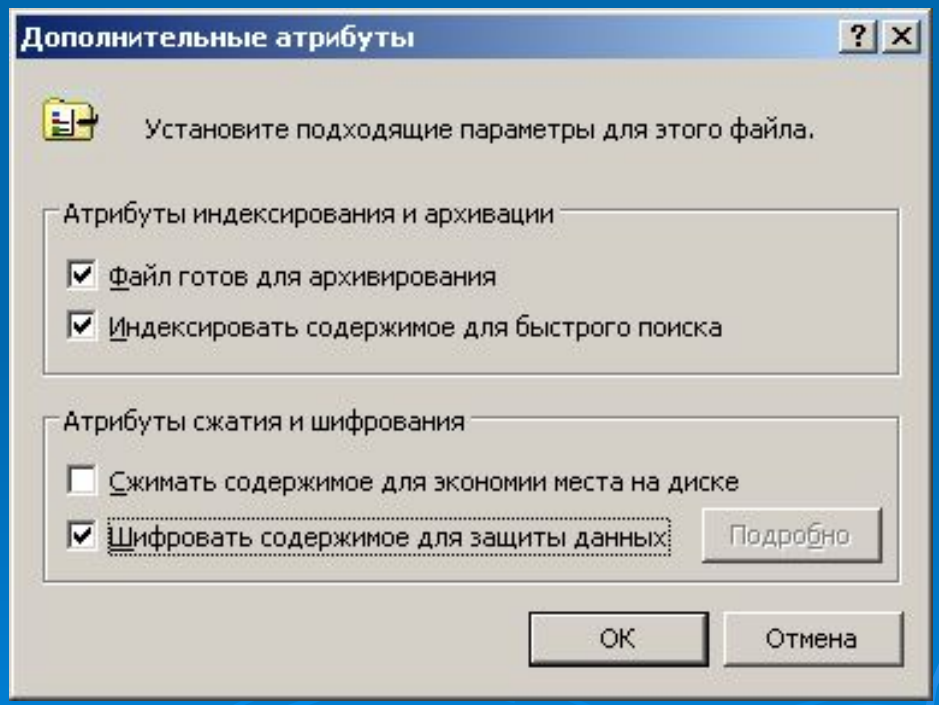
2. **В появившемся окне свойств на вкладке *Общие (General)* нажмите кнопку *Другие (Advanced).* Появится диалоговое окно *Дополнительные атрибуты (Advanced Attributes).***

3. **В группе *Атрибуты сжатия и шифрования (Compress or Encrypt attributes)* установите флажок *Шифровать содержимое для защиты данных (Encrypt contents to secure data)* и нажмите кнопку ОК.**

4. **Нажмите кнопку *ОК* в окне свойств зашифровываемого файла или папки. В появившемся диалоговом окне подтвердите режим шифрования.**

При шифровании папки можно указать следующие режимы:

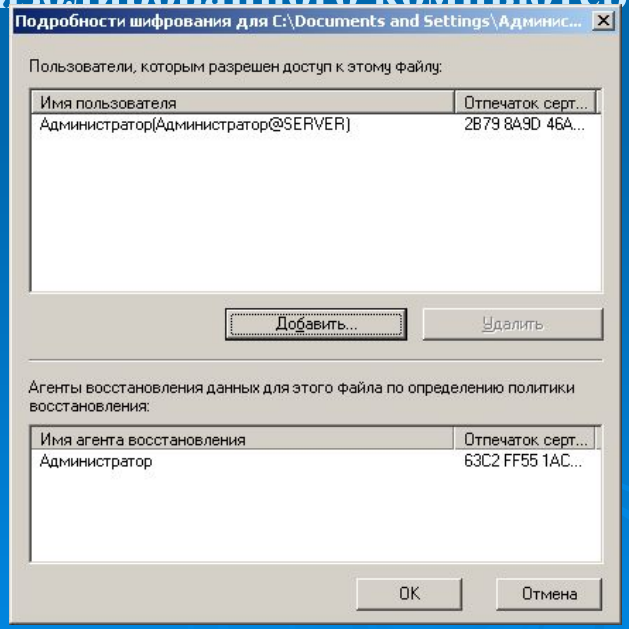
- **Только к этой папке (*Apply changes to this folder*).**
- **К этой папке и всем вложенным папкам и файлам (*Apply changes to this folder, subfolders and files*).**



Шифрование файлов для совместного использования

Windows XP, в отличие от ***Windows 2000***, поддерживает совместный доступ к зашифрованным *файлам*, расположенным на общих сетевых ресурсах в домене на базе Active Directory или на локальных дисках. Дополнительные разрешения нужно давать для каждого файла *индивидуально.*

После того как владелец-создатель зашифровал файл, он может снова открыть окно *Дополнительные атрибуты (Advanced Attributes)* и нажать кнопку *Подробно (Details)*. Появится окно, аналогичное показанному на рисунке (для изолированного компьютера картина будет аналогичной).

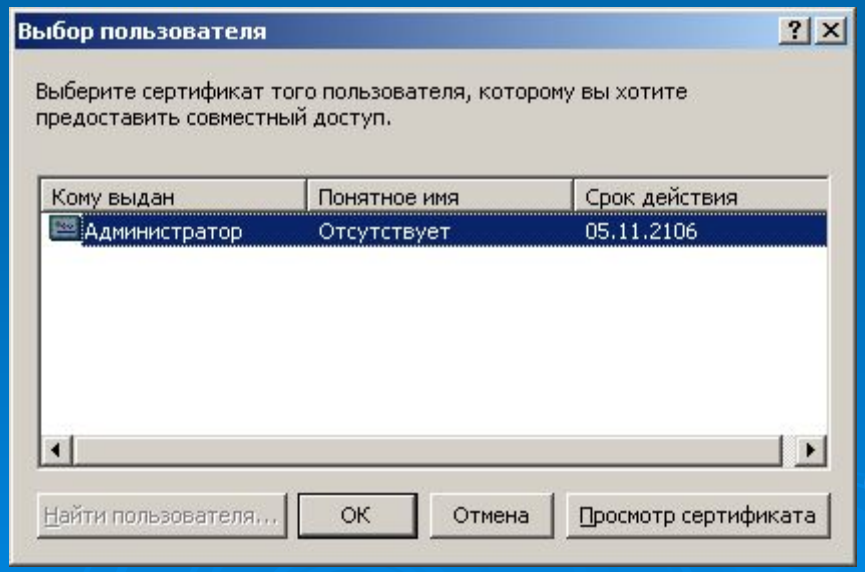


В приведенном примере видно, что к файлу помимо агента восстановления имеют доступ еще два пользователя.

Зашифровав файл или папку и открыв заново окно *Подробности шифрования (Encryption Details)*, вы можете легко проверить, определен ли в вашей системе агент восстановления.

Теперь можно нажать кнопку *Добавить (Add)* и в окне *Выбор пользователя (Select User)* указать, какие пользователи смогут также работать с зашифрованным файлом.

Окно *Выбор пользователя (Select User)* позволяет просмотреть имеющиеся сертификаты пользователей или найти пользователей в каталоге *Active Directory*.



Дешифрование файлов и каталогов

1. Чтобы дешифровать файл или папку, на вкладке *Общие (Sharing)* окна свойств соответствующего объекта нажмите кнопку *Другие (Advanced).*

2. В открывшемся окне диалога в группе *Атрибуты сжатия и шифрования (Compress or Encrypt attributes)* сбросьте флажок *Шифровать содержимое для зашиты данных (Encrypt contents to secure data).*

Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок

Операции копирования, перемещения, переименования и уничтожения зашифрованных файлов и папок выполняются точно так же, как и с незашифрованными объектами. Однако следует помнить, что пункт назначения зашифрованной информации должен поддерживать шифрование (должен иметь файловую систему NTFS 5.0). В противном случае при копировании данные будут расшифрованы, и копия будет содержать открытую информацию.

Архивация зашифрованных файлов

Резервную копию зашифрованного файла можно создать с помощью простого копирования его на другой жесткий диск или с использованием утилиты архивации. Однако, простое копирование, например, на дискету или оптический диск *может* привести к тому, что резервная копия будет содержать открытые данные. То есть, если скопировать зашифрованный файл на раздел FAT или на дискету, копия будет не зашифрована и, следовательно, доступна для чтения любому пользователю.

Специализированная операция архивации не требует для ее выполнения доступа к открытым ключам пользователя — только к архивируемой информации. Поэтому для обеспечения безопасности конфиденциальных данных при создании резервных копий рекомендуется применять специальные утилиты архивации. В Windows XP для этих целей предназначена стандартная утилита архивации данных *Backup*.

В процессе архивации зашифрованные данные будут скопированы на указанный носитель без дешифрования. Целевой носитель может не поддерживать NTFS 5.0. Например, резервная копия зашифрованных файлов может быть создана на гибком диске.

Управление сертификатами пользователей

Пользователи могут запрашивать, экспортировать, импортировать сертификаты, служащие в *EFS* для идентификации пользователей, а также управлять ими. Эта возможность предназначена для опытных пользователей, которые хотят иметь средство управления собственными сертификатами. Обычно пользователям не приходится самостоятельно управлять сертификатами, поскольку *EFS* автоматически генерирует для них пару ключей при первом обращении к ней — т. е. при попытке зашифровать файл или каталог (при этом открытый ключ сертифицируется в центре сертификации, а если таковой недоступен, то *EFS* сама подписывает открытый ключ).

В вышесказанном легко убедиться, если после инсталляции системы запустить оснастку *Сертификаты (Certificates)* и раскрыть узел (папку) *Личные (Personal)*: этот узел будет пуст. Если затем зашифровать некоторый файл или папку и вернуться в оснастку *Сертификаты (Certificates)*, то можно увидеть, что в папке *Личные (Personal)* появился сертификат, выданный текущему пользователю.

Управление сертификатами, их импорт и экспорт осуществляется с помощью контекстных меню оснастки *Сертификаты (Certificates)*. Пользователи имеют возможность управлять только своими собственными сертификатами

Восстановление зашифрованных файлов на другом компьютере

Часто возникает необходимость восстановить зашифрованную информацию *не на том* компьютере, на котором она была заархивирована. Это можно выполнить с помощью утилиты архивации, которая сохраняет информацию в зашифрованном виде вместе с атрибутом шифрования. Однако нужно позаботиться о переносе на новый компьютер соответствующего сертификата и личного ключа пользователя либо с помощью перемещаемого профиля, либо вручную.

На любом компьютере, где зарегистрировался пользователь, обладающий перемещаемым профилем, будут применяться одни и те же ключи шифрования.

Ручной перенос личного ключа и сертификата выполняется в два этапа: сначала следует создать резервную копию сертификата и личного ключа, а затем восстановить созданную копию на другом компьютере. (Эта процедура имеет смысл только для компьютеров, не входящих в домен. В домене можно использовать процедуру, описанную выше *"Шифрование файлов для совместного доступа".)*

Создание резервной копии сертификата (экспорт сертификата) состоит из следующих шагов:

1. **Запустите оснастку *Сертификаты (Certificates)*.**

2. **В левом подокне оснастки *Сертификаты* откройте папку *Личные (Personal)*, а затем папку *Сертификаты*. В правом подокне появится список ваших сертификатов.**

3. **Укажите переносимый сертификат и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду *Все задачи (All Tasks)*. В ее подменю выберите команду *Экспорт (Export)*. Запустится *Мастер экспорта сертификатов* (Certificate Export Wizard).**

4. **Нажмите кнопку *Далее (Next)*.**

5. **В следующем окне мастера выберите опцию *Да, экспортировать закрытый ключ (Yes, export the private key)*. Затем нажмите кнопку *Далее (Next)*.**

6. В следующем окне мастера доступен только один формат (*PFX*), предназначенный для персонального обмена информацией. Нажмите кнопку *Далее (Next)*.

7. В следующих окнах введите произвольный пароль, защищающий данные файла **.pfx*, а также путь для сохранения файла **.pfx*; затем нажмите кнопку *Далее (Next)*.

8. Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку *Готово (Finish)*.

9. Завершите работу мастера экспорта нажатием кнопки *ОК* в окне диалога, сообщающем об успешном выполнении процедуры экспорта.

Операцию экспорта может выполнить только сам пользователь. Даже администратор не может экспортировать личный ключ другого пользователя (хотя он и может экспортировать все сертификаты, хранящиеся на компьютере — но без личных ключей).

В результате сертификат и секретный ключ будут экспортированы в файл с расширением *pfx*, который может быть скопирован на гибкий диск и перенесен на другой компьютер.

Для восстановления сертификата из резервной копии:

1. Перенесите созданный на предыдущем этапе файл с расширением *pfx* на компьютер, где вы планируете восстанавливать зашифрованные данные.

2. Запустите оснастку *Сертификаты (Certificates)*.

3. В окне структуры оснастки *Сертификаты* откройте папку *Личные (Personal)*, затем папку *Сертификаты*. В правом подокне появится список ваших сертификатов.

4. Щелкните правой кнопкой мыши на пустом месте правого подокна. В появившемся контекстном меню выберите команду *Все задачи (All Tasks)*. В ее подменю выберите команду *Импорт (Import)*. Запустится *Мастер импорта сертификатов* (*Certificate Import Wizard*).

5. Следуйте указаниям мастера — укажите местоположение файла с расширением *pfx* и сообщите пароль защиты данного файла. Восстановление данных из резервной копии должно быть выполнено в папку *Личные (Personal)*.

6. Для начала операции импорта нажмите кнопки *Готово (Finish)* и *ОК*. После завершения процедуры импорта нажмите кнопку *ОК* и закройте окно мастера импорта.

В результате текущий пользователь получит возможность работать с зашифрованными данными на этом компьютере.

Утилита Cipher

В системах *Windows XP Professional* для шифрования/дешифрования файлов и папок можно также использовать утилиту командной строки Cipher.

Эта утилита командной строки позволяет шифровать и дешифровать файлы. Ниже приведен ее синтаксис, описание параметров дано в таблице 1.

```
cipher [/E|D] [/S:каталог] [/A] [/I] [/F] [/Q] [/H] [путь [...]]›
cipher /K
cipher /R:<имяфайла>
cipher /U [/N]
cipher /W:<имяПапки>
```

Таблица 1. Параметры утилиты cipher

Параметр	Описание
/E	Шифрует указанные папки. Эти папки помечаются как зашифрованные, все файлы, которые будут помещены в них впоследствии, шифруются автоматически
/D	Дешифрует все указанные после ключа файлы. Каталоги помечаются как незашифрованные — все файлы, которые будут помещены в них впоследствии, шифроваться не будут
/S	Выполняет заданную операцию с указанной папкой и входящими в нее подпапками
/A	Выполняет определенную ключом операцию как для папок, так и для файлов
/I	Продолжает выполнение указанной операции даже после возникновения ошибочной ситуации. По умолчанию при появлении ошибки программа Cipher останавливается
/F	Осуществляет принудительное шифрование всех файлов, указанных после ключа, даже если они уже зашифрованы. По умолчанию уже зашифрованные файлы не подвергаются вторичному шифрованию
/Q	Выдает только краткую информацию
/H	Отображает файлы, для которых установлены атрибуты ***скрытый*** **(Hidden) и** ***системный*** **(System)**

Таблица 1 (продолжение). Параметры утилиты cipher

/К	Создает новый ключ для пользователя, запустившего команду; при этом все другие параметры команды игнорируются
/R	Создает личный ключ и сертификат агента восстановления **EFS** для пользователя, запустившего команду
/N	Запрещает обновление ключей. Используется только с параметром **/n** для поиска всех зашифрованных файлов на локальных дисках
/U	Обращается ко всем зашифрованным файлам, при этом для них обновляются ключи шифрования и агента восстановления. Может использоваться только с параметром **/N**
/W	Стирает всю информацию в неиспользуемом дисковом пространстве; при этом все другие параметры команды игнорируются

Параметр путь может быть маской, файлом или папкой. Команда cipher без параметров выдает информацию о том, зашифрована ли данная папка или файлы, находящиеся в ней. Если параметр путь присутствует, то имен файлов может быть несколько. Между собой параметры должны быть разделены пробелом.

Для того чтобы зашифровать каталог *Мои документы (My Documents)*, введите команду:

```
c:\cipher /E  "Мои документы"
```

Для того, чтобы зашифровать все файлы с расширением doc, введите команду:

```
c:\cipher /E /A *.doc
```

Практическая часть

1) Создайте сертификат, пригодный для импорта.
2) Изучите работу утилиты cipher.

Результат: Выполнив работу, вы научитесь использовать EFS и cipher для шифрования данных.