Тема: 3.5 Аппаратное и программное обеспечение защищенных компьютерных систем.

Учебные вопросы:

1. Шифрование файлов и папок пользователя с использованием файловой системы EFS.
2. Создание и использование электронной цифровой подписи средствами операционной системы.

1. Шифрование файлов и папок пользователя с использованием файловой системы EFS

Краткие теоретические сведения:

Файловая система EFS: общие сведения

Шифрование – это процесс преобразования данных в формат, недоступный для чтения другим пользователям. После того как файл был зашифрован, он автоматически остается зашифрованным в любом месте хранения на диске.

Расшифровка (*дешифрование)* – это процесс преобразования данных из зашифрованной формы в его исходный формат.

Существует целый набор программных продуктов, обеспечивающих шифрование данных с помощью образованного от пароля ключа на уровне приложений (так называемое «закрытое», или «непрозрачное» шифрование). Однако такой подход имеет ряд ограничений (уязвимостей):

1) *Пользователю приходится расшифровывать файл перед каждым его использованием, а затем опять зашифровывать*. Если пользователь забывает зашифровать файл после окончания работы с ним, информация остается незащищенной. Поскольку каждый раз необходимо указывать, какой файл должен быть зашифрован (и расшифрован), применение такого метода защиты информации не только уязвимо, но и неудобно с практической точки зрения.

2) *Утечка информации из временных файлов и файлов подкачки*. Практически все приложения в процессе редактирования документов создают временные файлы. Они остаются на диске незашифрованными, несмотря на то что оригинальный файл зашифрован. Кроме того, шифрование информации на уровне приложений выполняется в режиме пользователя ОС. Это значит, что ключ, применяемый для такого типа шифрования, может храниться в файле подкачки. В результате, с помощью изучения данных файла подкачки можно получить ключ и расшифровать все документы пользователя.

3) *Слабая криптостойкость ключей*. Ключи образуются от паролей или случайных фраз. Поэтому в случае, если пароль был легко запоминаемым, атаки с помощью словарей могут легко привести к взлому системы защиты.

Все перечисленные выше проблемы позволяет решить так называемое «прозрачное» шифрование (шифрование «на лету»), реализованное с помощью шифрующей файловой системы EFS (Encrypting File System), являющейся встроенным компонентом ОС Windows (в версии выше 2000).

«Прозрачное» шифрование означает, что перед использованием файл не нужно расшифровывать. Можно, как обычно, открыть файл и изменить его. В системе прозрачного шифрования EFS криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Работает EFS следующим образом. Когда необходимо зашифровать файл система генерирует случайный ключ, называемый FEK (File Encryption Key). Этим ключом с помощью симметричного алгоритма шифрования кодируется файл. Симметричный – значит файл шифруется и расшифровывается одним ключом – FEK.

При первой необходимости шифрования информации ОС Windows создает два ключа пользователя: открытый и закрытый. FEK шифруется с помощью асимметричного алгоритма с использованием открытого ключа пользователя. Асимметричный алгоритм шифрования значит, что файл шифруется одним ключом (в нашем случае открытым), а расшифровывается другим (закрытым). Зашифрованный ключ FEK записывается рядом с зашифрованным файлом.

Закрытый ключ шифруется с помощью пароля пользователя. Поэтому защищенность вашей информации на прямую зависит от сложности вашего пароля. Поэтому и рекомендуется задать его более чем из 8-ми символов, включая буквы в нижнем и верхнем регистрах, цифры и специальные символы

Для расшифровки данных необходимо зайти под учетной записью пользователя, который зашифровал файлы. При этом автоматически при вводе правильного пароля расшифровывается закрытый ключ. С помощью последнего расшифровывается FEK (File Encryption Key), которым расшифровывается нужный файл.

Шифрование и расшифровывание файлов выполняется установкой свойств шифрования для папок и файлов, как устанавливаются и другие атрибуты, например «только чтение», «сжатый» или «скрытый». Если шифруется папка, все файлы и подпапки, созданные в зашифрованной папке, автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Шифрующая файловая система автоматически создает пару ключей шифрования для пользователя, если она отсутствует.

При работе с шифрующей файловой системой EFS следует учитывать следующие сведения и рекомендации:

1) Могут быть зашифрованы только файлы и папки, находящиеся на томах NTFS;

2) Сжатые файлы и папки не могут быть зашифрованы. Если шифрование выполняется для сжатого файла или папки, файл или папка преобразуются к состоянию без сжатия;

3) При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Однако обратная операция не приведет к автоматической расшифровке файлов. Файлы необходимо явно расшифровать;

4) Не могут быть зашифрованы файлы с атрибутом «Системный» и файлы в структуре папок системный корневой каталог;

5) Шифрование папки или файла не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы. Поэтому **возможности файловой системы шифрования EFS рекомендуется использовать совместно с системой соответствующего разграничения прав доступа**;

6) Процесс шифрование является прозрачным для пользователя.

Операции шифрования (дешифрования) можно выполнить двумя различными способами – используя графический интерфейс Windows Explorer (GUI) или консольную утилиту *Cipher*.

Шифрование (дешифрование) данных с помощью EFS (с использованием GUI)

Алгоритм действий по шифрованию файлов и папок с файлами с помощью EFS (с использованием GUI) состоит из следующих операций:

1. Вызовите контекстное меню защищаемого вами объекта и выберите команду «Свойства» (рис.1).

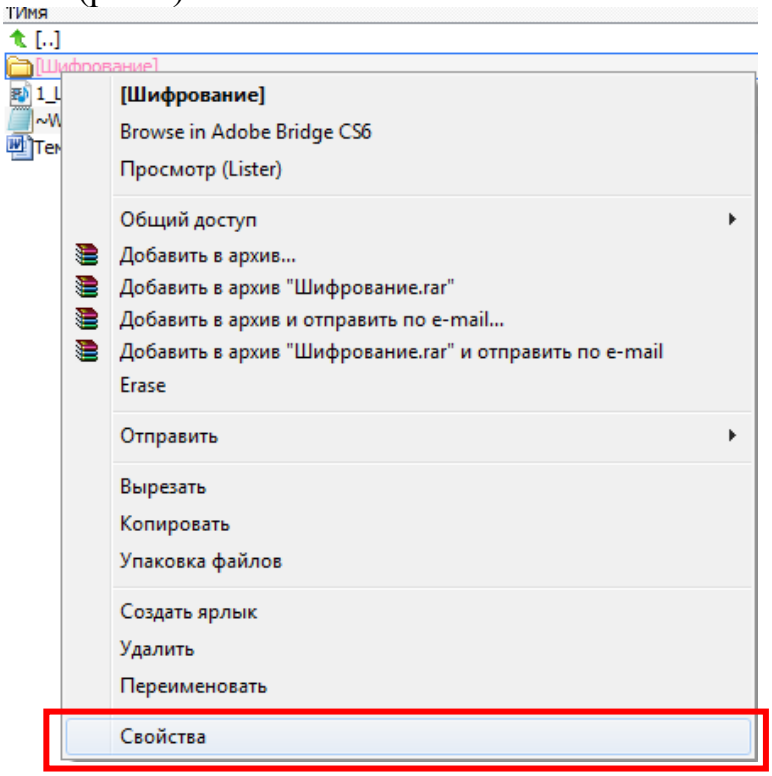

Рис. 1. Вызов контекстного меню для файла, выбранного для шифрования

2. Перейдите на вкладку «Общие» и нажмите кнопку «Другие» (рис. 2), что приведет к открытию окна «Дополнительные атрибуты» (рис. 3).

3. Активируйте параметр «Шифровать содержимое для защиты данных» (рис. 3).

4. Закройте открытые диалоговые окна при помощи кнопки «Ок».

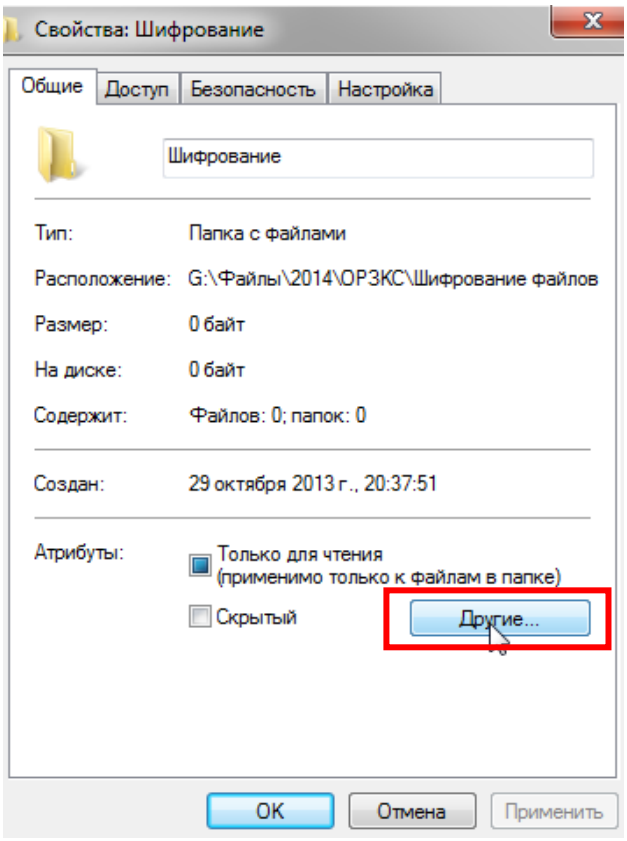

Рис.2. Выбор атрибутов «Другие» для файла, предназначенного для шифрования

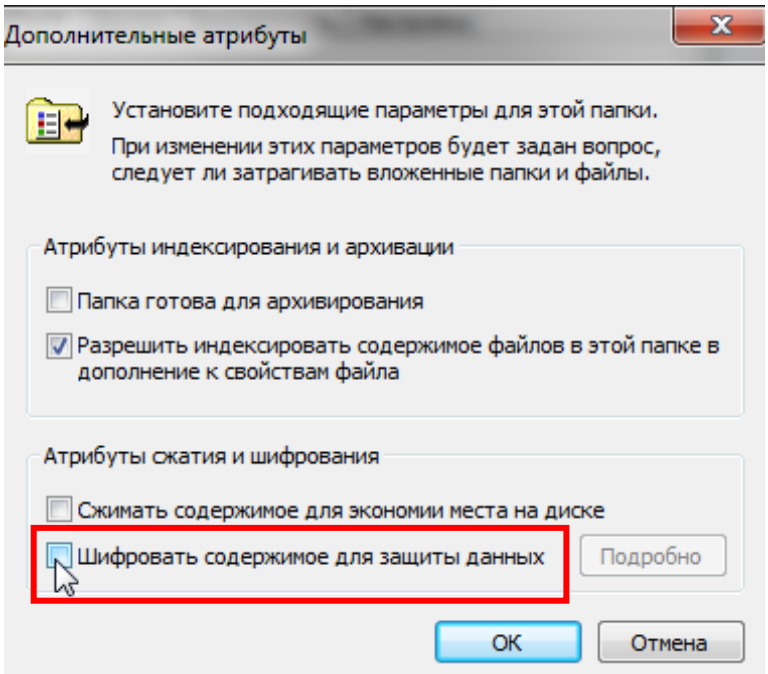

Рис.3. Установка атрибута шифрования

Если шифруется каталог (папка), система выдаст дополнительный запрос на запуск шифрования всего каталога (рис. 4). После того, как вы подтвердите свои намерения, все файлы будут зашифрованы.

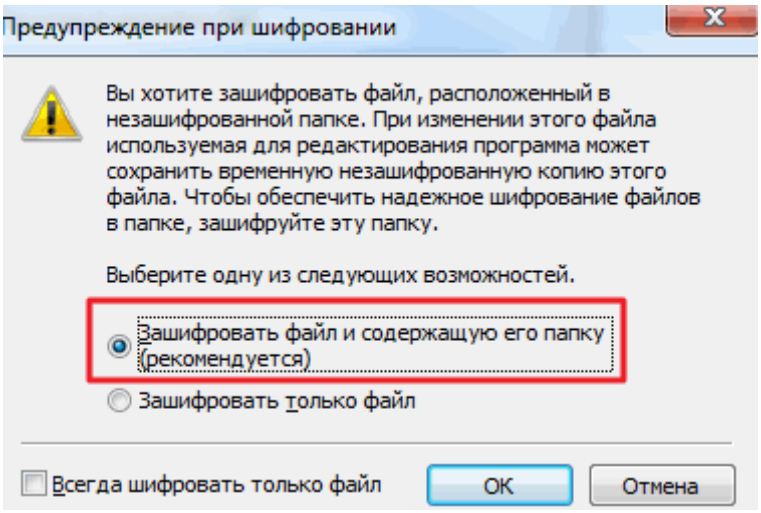

Рис.4. Дополнительный запрос на запуск шифрования всего каталога

Зашифрованные файлы обычно помечаются зеленым цветом (если это указано в настройках) (рис. 5).

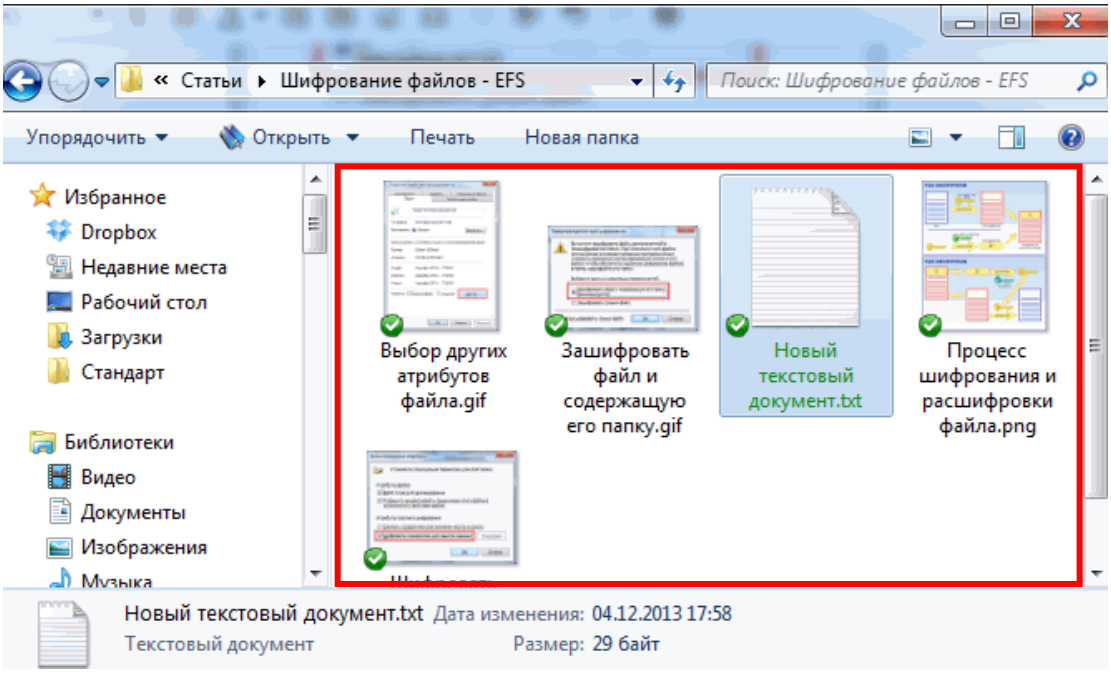

Рис.5. Зашифрованные файлы (обычно помечаются зеленым цветом)

5. Для того чтобы расшифровать зашифрованные файлы, нужно проделать обратную операцию: в контекстном меню защищенного объекта снять отметку «Шифровать содержимое для защиты», после чего нажать на кнопку «Ок».

Сохранение резервной копии сертификата EFS и ключей шифрования

Как только пользователь зашифровал какую-нибудь папку или файл, Windows создаст для данного пользователя (учетной записи) сертификат и связанную с ним пару ключей (открытый и секретный ключ), на основании которых будет происходить шифрование и дешифрование файлов. Сертификат – цифровой документ, используемый для проверки подлинности и безопасной передачи данных в общедоступных сетях, он связывает открытый ключ с объектом, содержащим соответствующий закрытый ключ.

Соответственно, эти сертификаты можно экспортировать для расшифровки данных на другом ПК.

Применительно к специфике рассматриваемого вопроса следует обратить внимание и на следующий аспект проблемы. Если некоторый пользователь или группа пользователей зашифровали файл с использованием EFS, то его содержимое доступно только им. Это приводит к рискам утери доступа к данным в зашифрованных файлах в случае утраты пароля данным пользователем (сотрудник забыл пароль, уволился и т.п.). Кроме того, при неблагоприятном стечении обстоятельств, пользователь может вообще потерять доступ к зашифрованным файлам. Это может произойти в следующих случаях:

а) аппаратные проблемы, например: вышла из строя материнская плата, испорчен загрузчик, повреждены системные файлы из-за сбоя жесткого диска. В итоге жесткий диск можно подключить к другому компьютеру, чтобы скопировать с него файлы, но если они зашифрованы с помощью EFS, они будут недоступны;

б) операционная система переустановлена. В этом случае доступ к зашифрованным данным будет также потерян;

в) удален профиль пользователя. Даже если создать пользователя с таким же именем, ему будет присвоен другой ID, и расшифровать данные все равно не получится;

г) системный администратор или сам пользователь сбросил пароль от своей учетной записи. После этого доступ к данным будет потерян.

Для предотвращения подобных проблем резервную копию сертификата EFS и ключей шифрования можно самостоятельно экспортировать с помощью консоли управления *mmc*. Алгоритм выполнения данной задачи состоит из следующих действий:

1. Запустите консоль *mmc* (Win+R > *mmc* > Enter).
2. В открывшейся консоли нажмите **CTRL+M** или перейдите в меню **Файл > Добавить или удалить оснастку…**
3. В открывшемся окне в разделе *Доступные оснастки* выберите **Сертификаты** и нажмите **Добавить >**.
4. Настройте оснастку для управления сертификатами вашей учетной записи и нажмите «Готово».

5. В окне «Добавление и удаление оснасток» нажмите на кнопку «Ок».

6. В дереве консоли слева перейдите по пути **Сертификаты > Личное > Сертификаты**. Выберите созданный сертификат и вызовите на нем контекстное меню. Раскройте раздел **Все задачи** и выберите **Экспорт…**

7. Откроется *Мастер экспорта сертификатов*. Для продолжения нажмите кнопку «Далее».

8. В открывшемся окне выберите значение «*Да, экспортировать закрытый ключ*» и нажмите кнопку «Далее».

Примечание: вы сможете экспортировать только свои ключи для расшифровки своих файлов. То есть, если другой пользователь для вас установил свой сертификат с ключами для расшифровки своих файлов, вы его закрытый ключ не сможете экспортировать.

9. В следующем окне *Мастера экспорта сертификатов* ничего не изменяйте и нажмите кнопку «Далее».

10. Задайте пароль для защиты экспортируемого сертификата.

11. Укажите расположение и имя экспортируемого файла.

12. В заключительном окне *Мастера экспорта сертификатов* нажмите кнопку «Готово». Экспорт сертификата будет успешно выполнен в файл *.pfx.

Примечание: для импорта сертификата на другом ПК достаточно запустить файл *.pfx и следовать инструкциям *Мастера импорта сертификатов*.

Создание агентов восстановления сертификата EFS и ключей шифрования

Для предотвращения вышеуказанных проблем, связанных с невозможностью доступа к зашифрованной информации, системный администратор может определить некоторые учетные записи в качестве агентов восстановления.

Агенты восстановления (*Recovery Agents*) определяются в политике безопасности **Encrypted Data Recovery Agents** (*Агенты восстановления шифрованных данных*) на локальном компьютере или в домене. Эта политика доступна через оснастку **Групповая политика** (*gpedit.msc*), в разделе «**Параметры безопасности > Политика открытого ключа > Файловая система EFS**». Пункт меню «**Действие > Добавить агент восстановления данных**» открывает мастер добавления нового агента.

Добавляя агентов восстановления, можно указать, какие криптографические пары (обозначенные их сертификатами) могут использовать эти агенты для восстановления шифрованных данных.

Шифрование (дешифрование) данных с помощью EFS (с использованием консольной утилиты Cipher)

Утилита командной строки CIPHER является альтернативным средством шифрования данных с помощью EFS. По сравнению с традиционным GUI она

обладает более широкими возможностями. Так, CIPHER отображает состояние шифрования текущего или указанного каталога и всех файлов в нем, может задавать различные режимы и параметры шифрования, создавать сертификаты и ключи с возможностью записи их на смарт-карту, выполнять шифрование или расшифровку файлов и каталогов, управлять доступом пользователей к зашифрованным данным, создавать агентов восстановления.

Ниже приведен общий синтаксис команды CIPHER. Описание ключей дано в табл. 1.

CIPHER [/E | D] [t/S:каталог] [/A] [/I] [/F] [/Q] [/H] [/K] [путь [...]]

Таблица 1. Ключи утилиты CIPHER

Ключ	Описание
/E	Шифрует указанные в качестве параметра *путь* файлы. Каталоги 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 каталогом *каталог* и всеми его подкаталогами, файлы при этом не обрабатываются
/A	Выполняет определенную ключом операцию как для каталогов, так и для отдельных 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)
/K	Создает новый ключ шифрования файлов для пользователя, запустившего команду; при этом все другие ключи команды игнорируются
/R	Создает ключ восстановления EFS и сертификат, затем записывает их в файл PFX (содержащий сертификат и закрытый ключ) и файл CER (содержащий только сертификат). Администратор может добавить содержимое файла CER в политику восстановления EFS для создания ключа восстановления для пользователей, а затем импортировать файл PFX для восстановления отдельных файлов.
/C	Отображает сведения о зашифрованном файле
/X	Создает резервные копии сертификата EFS и ключей и сохраняет их в файл.

Параметр *путь* может быть маской, файлом или каталогом. Команда CIPHER без параметров выдает информацию о том, зашифрован ли данный каталог или файлы, находящиеся в нем. Если параметр *путь* присутствует, то имен файлов может быть несколько. Между собой параметры должны быть разделены пробелом.

Как видно из таблицы 1, с помощью утилиты CIPHER можно создать (используя ключ **/R**) нового агента восстановления (ключ и сертификат). В этом случае CIPHER создаст два файла *.PFX и *.CER. В первом из них будет находиться сертификат и закрытый ключ, во втором – только сертификат.

Для активации агента восстановления в системе необходимо добавить созданный сертификат (CER) в политики (с помощью оснастки групповой политики *gpedit.msc*).

Используя ключ **/X,** можно создать резервную копию текущего сертификата шифрования. При этом имя файла запрашивается перед архивированием. По умолчанию, файл резервной копии сохраняется в домашнем каталоге пользователя и защищается паролем, вводимым пользователем по запросу программы.

Вышеуказанные действия следует проводить от лица пользователя, обладающего администраторскими привилегиями.

Рассмотрим некоторые примеры использования утилиты командной строки CIPHER.

Пример 1. Определить учетную запись, зашифровавшую файл printer.xlsx. Синтаксис команды будет выглядеть следующим образом:

```
cipher /c c:\SecretData\printer.xlsx
```

Результаты выполнения команды представлены на рис. 1.

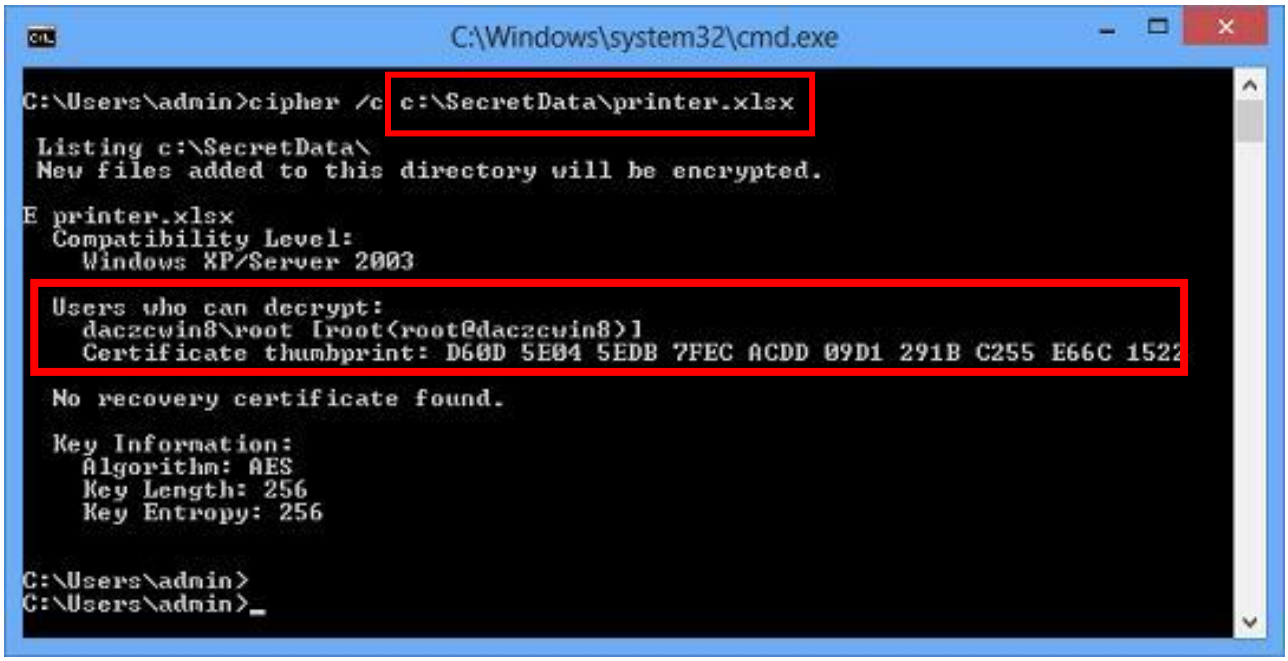

Рис.5. Зашифрованные файлы (обычно помечаются зеленым цветом)

Пример 2. Зашифровать подпапку CONF и все ее подпапки. Синтаксис команды будет выглядеть следующим образом:

```
cipher /e /s:D:\CONF
```

В ходе выполнения команды будет отображаться следующая справочная информация:

Шифрование файлов в D:\CONF
passwords [OK]
security [OK]
Шифрование файлов в D:\CONF\PASSWORDS
far.psw [OK]
. . .

Пример 3. Отобразить состояние шифрования для папки D:\CONF. Синтаксис команды будет выглядеть следующим образом:

cipher /s:D:\CONF

Пример отображаемой информации:

Список D:\CONF
Новые файлы, добавленные в эту папку, будут зашифрованы.
E passwords
E security
Список D:\CONF\PASSWORDS
Новые файлы, добавленные в эту папку, будут зашифрованы.
E far.psw
Список D:\CONF\SECURITY
Новые файлы, добавленные в эту папку, будут зашифрованы.
E diagerr.xml
E diagwrn.xml
. . .

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.3»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.

2. Создайте в системе новую пользовательскую учетную запись **User1** (тип учетной записи – *стандартная*). Для этого воспользуйтесь оснасткой **«Управление компьютером»** (*compmgmt.msc*).

При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля.

3. Создайте новую группу пользователей **«Group_test»** и включите в нее пользователя **User1**. Удалите пользователя **User1** из других групп.

4. Создайте на диске **C:** папку **TEST**. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt, *.doc и пр.).

5. Просмотрите разрешения прав доступа к папке **c:\TEST**.

6. Разрешите пользователю **User1** запись в папку **TEST**, но запретите запись для группы **Group_test**. Попробуйте записать файлы или папки в **TEST** от имени пользователя **User1**. В файл-отчете опишите результат. Просмотрите и проанализируйте действующие разрешения пользователя **User1** к папке **TEST** в окне свойств папки.

7. Используя стандартное окно свойств папки **TEST**, задайте для пользователя **User1** такие права доступа к папке, чтобы он мог записывать информацию в папку **TEST**, но не мог просматривать ее содержимое. Проверьте, что папка **TEST** является теперь для пользователя **User1** «невидимой». Для этого запустите от его имени файловый менеджер и выполните следующие действия: а) запишите файлы в папку; б) просмотрите ее содержимое; в) удалите файл из папки. В файл-отчете зафиксируйте результат.

8. В папке **TEST** создайте папку **Docs**. Для вложенной папки **TEST\Docs** отмените наследование ACL[1] от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя **User1** папка **TEST\Docs** перестала быть «невидимой» (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл с расширением *.xls).

9. Снимите запрет на чтение папки **TEST** для пользователя **User1**. Запретите этому пользователю доступ к файлам с расширением *.doc в папке **TEST**. Убедитесь в недоступности этих файлов для пользователя **User1**.

10. Запретите пользователю **User1** все права на доступ к папке **TEST** и разрешите полный доступ к вложенной папке **TEST\Docs**. Убедитесь в доступности папки **TEST\Docs** для пользователя **User1**. Опишите результат в файл-отчете.

11. Создайте в папке **TEST** новую папку **Encrypt**. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt, *.doc и пр.).

12. Зашифруйте папку **Encrypt** и все ее содержимое из меню свойств папки от имени администратора. Убедитесь, что после этого будет создан сертификат пользователя, запустив оснастку *certmgr.msc* от имени пользователя (раздел **Личные**). Просмотрите и зафиксируйте в файл-отчете основные параметры сертификата открытого ключа пользователя **User1** (срок действия, используемые алгоритмы).

13. Попробуйте просмотреть или скопировать какой-нибудь файл из папки **Encrypt** от имени пользователя **User1**. Зафиксируйте результат в файл-отчете.

14. Скопируйте зашифрованный файл в незашифрованную папку (например, **TEST**). Убедитесь, что он остался зашифрованным. Добавьте

[1] ACL (Access Control List) – список управления доступом, который определяет, кто или что может получать доступ к объекту, и какие именно операции разрешено или запрещено выполнять субъекту.

пользователя **User1** в список имеющих доступ к файлу пользователей. Повторите попытку получить доступ к файлу от имени пользователя **User1**.

15. Создайте учетную запись нового пользователя **User_agent**, сделайте его членом группы *Администраторы*. Определите для пользователя **User_agent** роль агента восстановления EFS.

16. Создайте в папке **TEST** новый текстовый файл с произвольным содержимым. Зашифруйте этот файл от имени пользователя **User1**. Убедитесь в окне подробностей шифрования файла, что пользователь **User_agent** является агентом восстановления для данного файла. Попробуйте прочитать содержимое файла от имени администратора и от имени пользователя **User_agent**. Опишите результат в файл-отчете.

17. С помощью консоли управления *mmc* экспортируйте на рабочий стол резервную копию сертификата EFS и ключей в PFX-файл под именем «Key_EFS».

18. С использованием консольной команды шифрования *Cipher* выполните следующие действия:

18.1. Зашифруйте все файлы с расширением *.doc в папке **TEST** и всех ее подпапках (предварительно снимите запрет на доступ к этим файлам, установленный в п. 9 настоящего задания).

18.2. Отобразите на экране состояние шифрования для папки **TEST\Docs**.

18.3. Сохраните резервную копию сертификата EFS и ключей в PFX-файл под именем «Key_EFS_rezerv» на рабочий стол.

Синтаксис выполненных команд *Cipher* опишите в файл-отчете.

19. Убедитесь, что при копировании зашифрованных файлов на том с файловой системой, не поддерживающей EFS (например, FAT32 на флеш-накопителе), содержимое файла дешифруется.

20. Обменяйтесь зашифрованными файлами по сети с коллегами. Попробуйте прочитать содержимое файлов, зашифрованных пользователями на других ПК. Самостоятельно выполните действия, необходимые для получения доступа к содержимому данных файлов. Опишите ваши действия и их результат в файл-отчете.

21. Продемонстрируйте работу и файл-отчет преподавателю.

22. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, удалите учетные записи **User1, User_agent**, а также группу **Group_test**.

23. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое шифрование? Что такое «прозрачное шифрование»?
2. Каким образом шифруются файлы в файловой системе EFS?
3. Какие алгоритмы шифрования используются в EFS?
4. Перечислите и охарактеризуйте функциональные особенности системы шифрования EFS.

5. Перечислите последовательность действий по работе с системой шифрования EFS для защиты конфиденциальной информации от несанкционированного доступа.

6. Для чего необходимо хранить резервную копию сертификата ключа шифрования системы EFS?

7. В каких случаях пользователь может потерять доступ к зашифрованным файлам?

8. С какой целью задается пароль на экспортируемую копию сертификата ключа шифрования системы EFS?

9. В чем преимущества использования командной строки и утилиты *Cipher* перед стандартным графическим интерфейсом GUI при шифровании файлов с помощью системы EFS?

2. Создание и использование электронной цифровой подписи средствами операционной системы

Краткие теоретические сведения:

Цифровые сертификаты электронной цифровой подписи: общие сведения

Электронная цифровая подпись (ЭЦП) – это набор символов (электронная зашифрованная печать), удостоверяющий подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы. ЭЦП подтверждает, что сведения предоставлены подписавшим их создателем и не были изменены.

Для создания ЭЦП необходим сертификат подписи, удостоверяющий личность. При отправке абоненту документа, подписанного ЭЦП, также отправляется сертификат и открытый ключ.

Как правило, сертификаты содержат следующие сведения:

а) значение открытого ключа субъекта;

б) сведения об идентификации субъекта, такие, как имя и адрес электронной почты;

в) срок действия (время, в течение которого сертификат считается действительным);

г) ЭЦП, заверяющая действительность связи между общим ключом субъекта и сведениями для его идентификации.

Для частного использования – чтобы организовать защищенный обмен данными по электронной почте либо по сети внутри замкнутого круга абонентов – совершенно не обязательно использовать услуги сертифицированных удостоверяющих центров. Для индивидуального использования ЭЦП гораздо удобнее выписывать самому себе самоподписанные сертификаты. В общем случае получателю для доверия к

сертификату будет достаточно, если отправитель подтвердит свою принадлежность к нему.

Таким образом, *личный сертификат* ЭЦП используется для подтверждения личности пользователя. Компонент цифровой подписи сертификата безопасности является электронной идентификационной карточкой пользователя и гарантирует следующие составляющие:

Подлинность. ЭЦП подтверждает личность подписавшего;

Целостность. ЭЦП подтверждает, что содержимое документа не было изменено или подделано после заверения;

Неотрекаемость. ЭЦП подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

Наличие ЭЦП указывает адресату, что сведения действительно поступили от указанного пользователя и не были перехвачены или подделаны.

Организация безопасного документооборота с использованием ЭЦП условно подразделяется нами на:

1) действия отправителя; 2) действия абонента (получателя электронных документов).

Рассмотрим их более подробно.

Действия отправителя. Создание личного сертификата ЭЦП. Подписание документа формата MS Word

Для того, чтобы создать сертификат с собственной цифровой подписью и подписать им текстовый документ формата MS Word, необходимо выполнить ряд следующих действий:

1. Запустите утилиту *Selfcert* (Win+R > *Selfcert* > Enter).

Примечание*:* утилита *Selfcert* создает сертификат с собственной подписью, который основывается на введенном имени и предназначен только для личного использования. Если для подписи широко распространяемых документов требуется заверенный сертификат на подпись, необходимо обратиться в специальный центр сертификации.

2. Введите имя сертификата (например, *Курсант Иванов*) и нажмите кнопку «Ок» (рис. 1). После выполнения данного действия появится сообщение об успешном создании ЭЦП.

3. Откройте документ MS Word, который необходимо подписать электронной цифровой подписью. Установите курсор в той части документа, где будет находится строка цифровой подписи.

4. Выполните команду **Меню Вставка > Строки подписи > Строка подписи MS Office**.

5. В открывшемся окне «Настройка подписи» введите Ф.И.О. автора подписи и иные данные (рис. 2). Для продолжения нажмите кнопку «Ок». После выполнения данного действия в соответствующем месте документа появится текстовое поле «Подпись» (рис. 3).

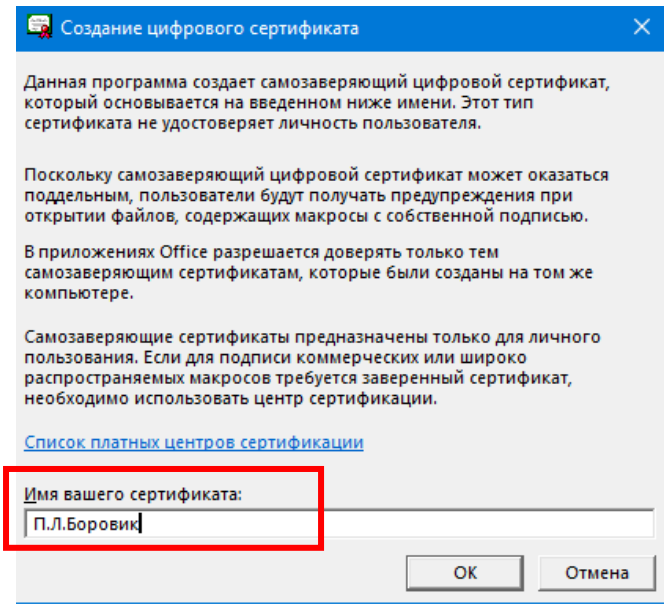

Рис.1. Создание ЭЦП

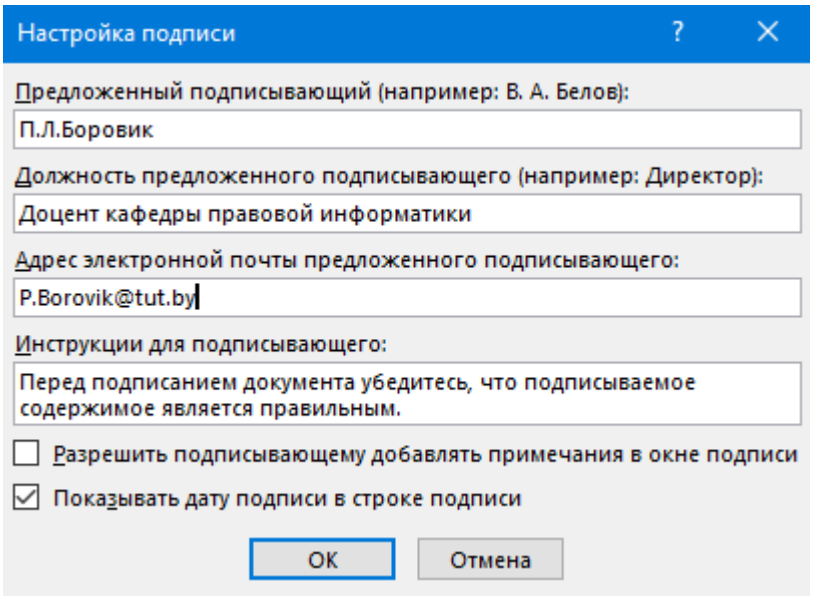

Рис.2. Настройка ЭЦП

Примечание: строка подписи напоминает типичный заполнитель подписи, который может выводиться в печатном документе. При вставке строки подписи в файл MS Office автор может указать сведения о предполагаемом подписавшего и инструкции для подписывающего. Когда электронная копия файла отправляется предполагаемому абоненту, этот пользователь видит строку подписи и уведомление о том, что его подпись запрашивается. Подписавший может:

ввести подпись;

выбрать изображение подписи от руки;

ввести подпись с помощью функции рукописного ввода на ПК с сенсорным экраном.

Одновременно с видимой подписью в документ добавляется и цифровая подпись для подтверждения личности подписавшего.

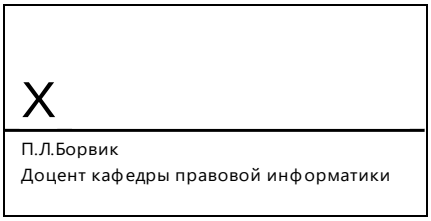

Рис.3. Текстовое поле ЭЦП в подписываемом документе MS Word

Для добавления дополнительных строк подписи указанные действия необходимо повторить.

6. Нажмите на строку подписи в файле правой кнопкой мыши. Выберите в меню команду *Подписать* (рис. 4).

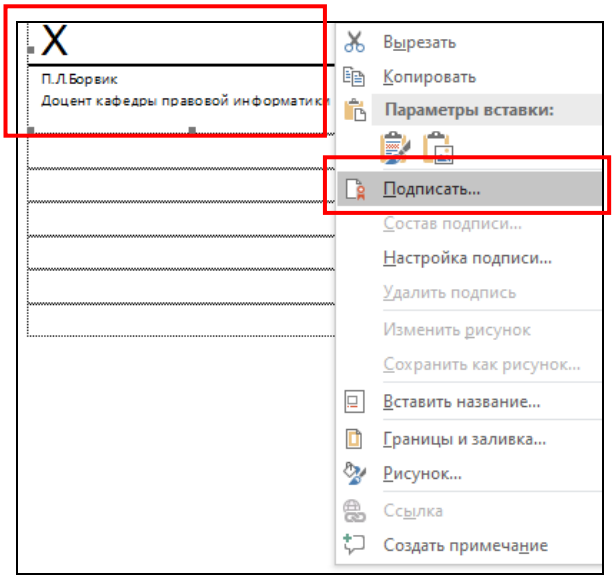

Рис.4. Подписание документа

7. Введите свое имя в поле рядом со значком X, чтобы добавить печатную версию подписи (рис. 5).

Нажмите кнопку «Выбрать рисунок», чтобы выбрать изображение своей рукописной подписи. В диалоговом окне «Выбор графической подписи» найдите файл, содержащий изображение подписи, выберите его и нажмите кнопку на «Выбрать».

8. Нажмите на кнопку «*Подписать*».

В нижней части документа или листа появится кнопка «Подписи», а в верхней части – кнопка «Просмотр подписей…» (рис. 6), при нажатии на которую откроется окно с информацией об ЭЦП (рис. 7).

Примечание: документ, подписанный цифровой подписью, становится доступен только для чтения.

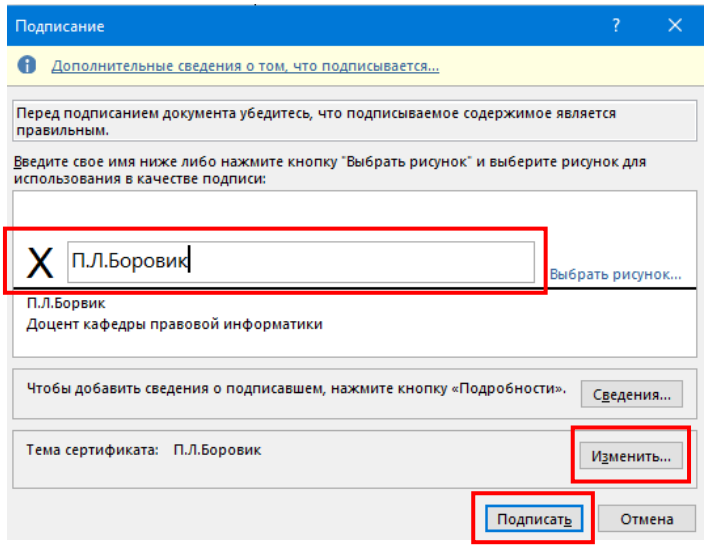

Рис.5. Подписание документа

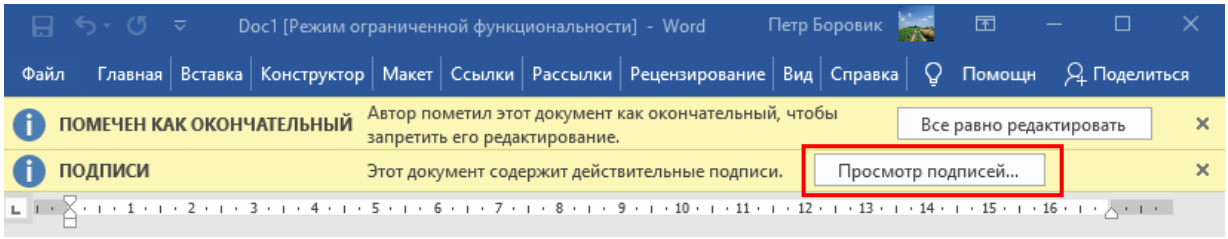

Рис.6. Создание ЭЦП

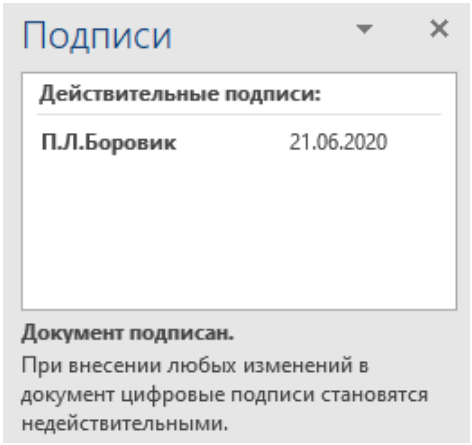

Рис.7. Создание ЭЦП

Экспорт сертификата открытого ключа ЭЦП

Для того, чтобы получатель ваших электронных документов был уверен в том, что документ действительно подписан вами, а в него после подписания не внесены несанкционированные изменения, он должен получить от вас и установить на свой компьютер *сертификат открытого ключа* вашей ЭЦП.

Для того, чтобы экспортировать из вашей системы *сертификат открытого ключа* ЭЦП, необходимо выполнить следующие действия:

1.Откройте консоль управления *mmc* (Win+R > *mmc* > Enter).

2. В окне «Добавление и удаление оснасток» добавьте новую оснастку «Сертификаты» (**Файл > Добавить или удалить оснастку**).

3. В дереве консоли слева перейдите по пути **Сертификаты > Личное > Сертификаты**. Выберите созданный сертификат (например, *Курсант Иванов*) и вызовите на нем контекстное меню. Раскройте раздел **Все задачи** и выберите **Экспорт…**

4. Откроется *Мастер экспорта сертификатов*. Для продолжения нажмите кнопку «Далее».

5. В открывшемся окне выберите значение «*Нет, не экспортировать закрытый ключ*» и нажмите кнопку «Далее».

6. В следующем окне *Мастера экспорта сертификатов* ничего не изменяйте и нажмите кнопку «Далее».

7. Укажите расположение и имя экспортируемого файла.

8. В заключительном окне *Мастера экспорта сертификатов* нажмите кнопку «Готово». Экспорт сертификата будет успешно выполнен в файл *.cer.

Действия получателя документов, подписанных ЭЦП

Для того, чтобы получатель ваших электронных документов установил на свой компьютер полученный от вас сертификат открытого ключа вашей ЭЦП (это единоразовое действие), ему необходимо выполнить следующие действия:

1. Установите полученный от отправителя сертификат его открытого ключа *.cer. Для этого правой кнопкой мыши нажмите на файл открытого ключа и в контекстном меню выберите пункт «Установить сертификат».

Запустится *Мастер импорта сертификатов*.

2. Следуйте указаниям мастера, а после завершения процедуры импорта нажмите кнопку «Ок» и закройте окно мастера импорта.

В результате указанных действий данный пользователь получит на своем компьютере возможность удостоверяться в подлинности вашей ЭЦП, которой вы будете подписывать свои документы.

3. Для того, чтобы получателю ваших документов, подписанных созданной вами ЭЦП, удостовериться в подлинности последней, ему необходимо открыть ваш документ. В нижней части документа или листа появится кнопка «Подписи», а в верхней части – кнопка «Просмотр подписей…» (рис. 6), при нажатии на которую откроется окно с информацией об ЭЦП.

Использование хеш-функций для удостоверения подлинности и целостности защищаемой информации

Альтернативным и, вместе с тем, наиболее универсальным способом удостоверения подлинности и целостности файла (документа, образа, текстового сообщения и пр.) является *хеширование* – криптографическое преобразование входных данных по определенному алгоритму в битовую строку определенной длины. При этом полученный в ходе вычислений

результат, представленный в шестнадцатеричной системе исчисления (например, *016f8e458c8f89ef75fa7a78265a0025*), называется *хешем* или *хеш-суммой*, *хеш-кодом*, *контрольной суммой, дайджестом, «цифровым отпечатком»*.

При этом в основе хеширования лежит односторонний метод вычисления. Обратное вычисление (расшифровку) произвести не представляется возможным, поскольку существующие стандарты хеширования не шифрует данные в прямом смысле этого слова, а вычисляет значение хеш-функции для заданного набора данных. Например, используя стандарт MD5 для текстовых данных длиной 1000 символов, пользователь получает дайджест из 32 цифр. Далее, для гипотетической расшифровки дайджеста нужно по имеющимся 32 символам определить какие именно 1000 символов были использованы, но это не реально даже с учётом того, что известно, что их было именно 1000, а не 3000 или 25. Поэтому взлом хеша не имеет никакого смысла.

Процесс хеширования широко применяется в программировании, веб-индустрии и информационной безопасности. Указанные области применения охватывают следующие основные направления:

создание ЭЦП;

защищенное хранение паролей в базах данных информационных систем;

создание криптографических ключей;

проверка подлинности и целостности элементов файловой системы ПК;

создание уникальных идентификаторов и др.

Так, в некоторых системах управления веб-сайтами (CMS) хеширование используется при организации хранения паролей учетных записей, номеров банковских кредитных карт и другой критически важной информации в базах данных (MySQL, MongoDB и др.). В случае взлома злоумышленниками таких баз к ним в руки попадёт только бесполезный набор символов.

Кроме того, хеш-код может использоваться и как контрольная сумма для сравнения файлов. Полное совпадение хеша означает идентичность сравниваемых файлов, то есть у двух различных файлов не может быть одинаковых хешей. Поэтому алгоритмы хеширования часто используется в различных файлообменных сетях, торрентах, архиваторах, при создании резервных копий, а также для организации защищенного документооборота.

Существуют различные алгоритмы хеширования (SHA-1, SHA-256, SHA-512, MD5 и др.), реализованные в виде как специальных программ, так и он-лайн сервисов.

Так, чтобы получить хеш одного из наиболее распространенных и устойчивых к взлому стандартов хеширования из любых имеющихся данных (текст, строки, файл), рекомендуется воспользоваться он-лайн сервисом, например: SNIPP.RU (https://snipp.ru/tools/md5-file) (рис. 8).

Алгоритм действий по созданию хэша достаточно прост: выбрать способ (функцию) хеширования, загрузить файл либо скопировать в специальное окно

текстовое сообщение, нажать на кнопку «Отправить», скопировать в буфер обмена полученный дайджест.

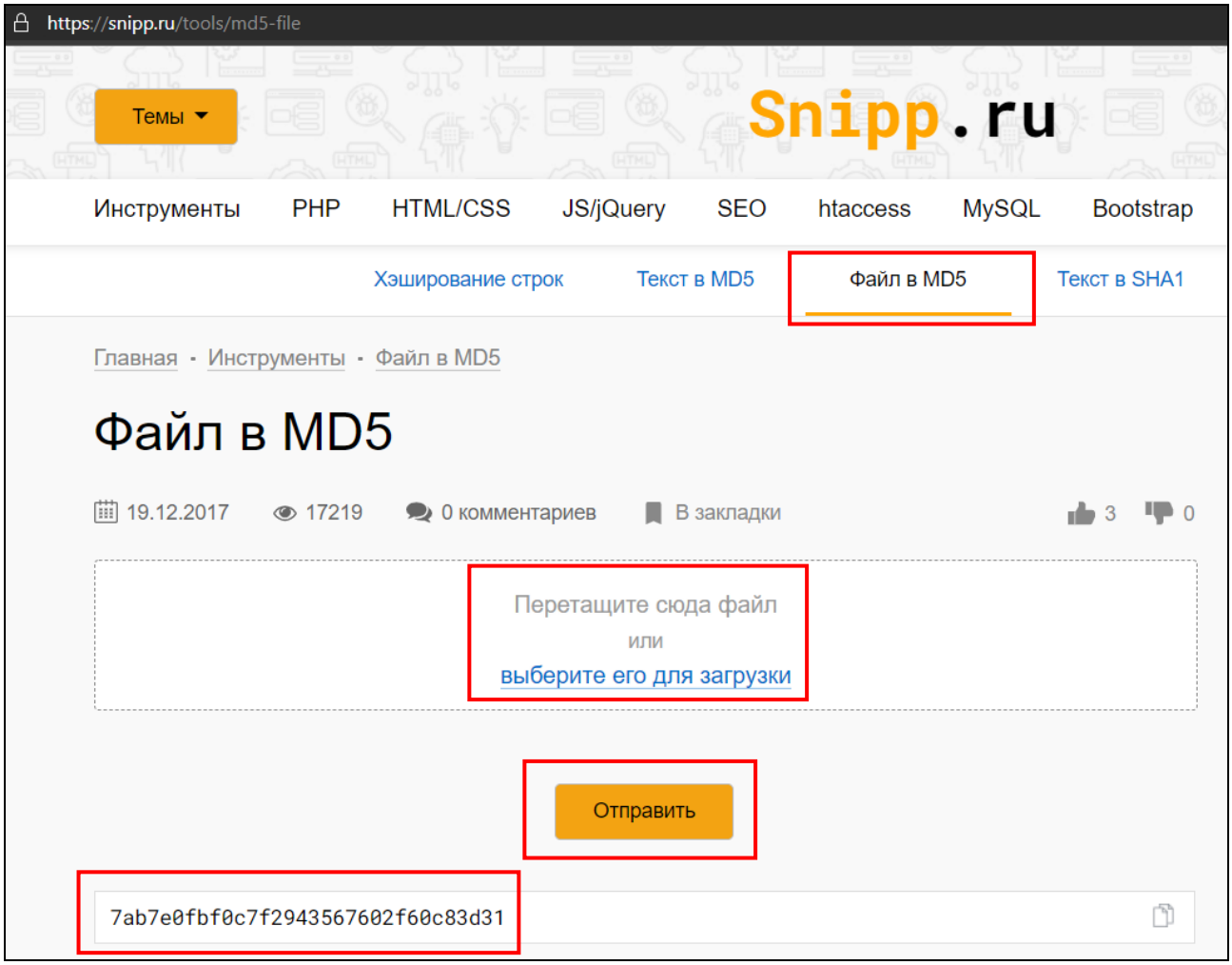

Рис. 8. Сервис для получения хеша файлов онлайн (https://snipp.ru/tools/md5-file)

Осуществить просмотр хэша любого файла можно и без какого-либо стороннего программного обеспечения, используя встроенный инструмент *PowerShell* для Windows. Для этого необходимо открыть окно *PowerShell* (Пуск > Windows PowerShell) и в командной строке выполнить следующую команду:

Get-FileHash [*путь к файлу*] [*алгоритм*]

Например:

Get-FileHash C:\path\to\file.iso

По умолчанию команда представит значение хеша стандарта SHA-256 для файла (рис. 9).

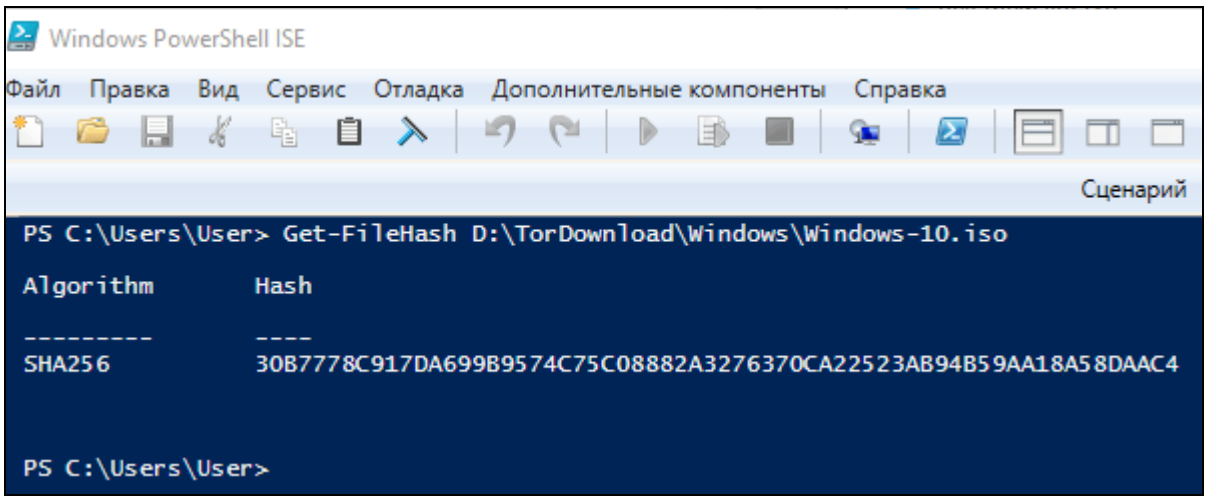

Рис. 8. Сервис Windows PowerShell, используемый для получения хеша файлов

Однако, в аргументе команды можно напрямую задать следующие алгоритмы хеширования: MD5, SHA1, SHA256, SHA384, SHA512, MACTripleDES, RIPEMD160

Например:

```
Get-FileHash C:\path\to\file.iso -Algorithm MD5
```

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Создайте новый сертификат с собственной цифровой подписью и подпишите:
   2.1. Текстовый документ формата MS Word.
   2.2. Электронную таблицу MS Excel.
   2.3. Файл базы данных MS Access.
3. Экспортируйте сертификат открытого ключа и передайте его по локальной сети своему коллеге для установки на своем компьютере.
4. После того, как ваш коллега установит сертификат вашего открытого ключа, передайте ему документы, подписанные созданной вами электронной цифровой подписью. Получатель ваших электронных документов должен удостовериться в подлинности ЭЦП.
5. Получите также от своих коллег сертификаты их открытых ключей и установите на своем компьютере. Получите от них файлы, подписанные цифровыми подписями, созданными ими. Удостоверьтесь в их подлинности. Результаты зафиксируйте в файл-отчете.
6. С использованием он-лайн сервиса SNIPP.RU (https://snipp.ru/tools/md5-file) удостоверьтесь в подлинности и целостности

файлов, полученных в п. 5 задания. Алгоритм действий каждого из участников документооборота подробно опишите в файл-отчете.

7. Повторите выполнение п. 6 задания с учетом следующих условий:

а) для проверки дайджеста используйте встроенной инструмент *PowerShell* для Windows;

б) при создании хэша файлов используйте алгоритм хеширования MD5.

Экранные копии полученных результатов (включая синтаксис используемой функции *Get-FileHash*) зафиксируйте в файл-отчете.

8. Осуществите поиск в сети «Интернет» альтернативных он-лайн генераторов хеш-кодов. Убедитесь в их работоспособности. Выполните сравнительный анализ. Результаты зафиксируйте в файл-отчете (с указанием URL-адреса найденного он-лайн сервиса, функциональных особенностей, преимуществ и недостатков).

9. Осуществите поиск в сети «Интернет» ссылок на описания существующих стандартов хеширования. Выполните их сравнительный анализ. Результаты зафиксируйте в файл-отчете.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое электронная цифровая подпись? Какие основные функции она выполняет?
2. Какие действия следует предпринять для организации безопасного документооборота с использованием электронной цифровой подписи?
3. Чем обеспечивается безопасность документооборота при использовании электронной цифровой подписи?
4. Что такое хэш-функция? Какие стандарты хеширования вы знаете?
5. Объясните механизм процесса хеширования. Приведите примеры. Расскажите о способах хеширования.