**Задание на лабораторную работу 2**

**по дисциплине “Безопасность ОС”**

***тема: Шифрование в ОС Windows***

Начиная с Windows 2000, в операционных системах семейства Windows (кроме домашних версий) возможно использование системы шифрования данных **Encrypting File System (EFS)**, реализующей шифрование на уровне файловой системы NTFS для защиты конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру или носителю информации. EFS использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре ”открытый / закрытый” ключ. По умолчанию закрытый ключ пользователя защищён паролем, и защищённость данных зависит от стойкости пароля пользователя.  
  
Утилита командной строки CIPHER отображает состояние шифрования текущего или указанного каталога и всех файлов в нем, может задавать 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.   
  
Форматы командной строки:   
  
**CIPHER [/E | /D | /C] [/S:directory] [/B] [/H] [pathname [...]]  
  
CIPHER /K [/ECC:256|384|521]   
  
CIPHER /R:filename [/SMARTCARD] [/ECC:256|384|521]   
  
CIPHER /P:filename.cer  
  
CIPHER /U [/N]   
  
CIPHER /W:directory  
  
CIPHER /X[:efsfile] [filename]   
  
CIPHER /Y  
  
CIPHER /ADDUSER [/CERTHASH:hash | /CERTFILE:filename | /USER:username] [/S:directory] [/B] [/H] [pathname [...]]  
  
CIPHER /FLUSHCACHE [/SERVER:servername]   
  
CIPHER /REMOVEUSER /CERTHASH:hash [/S:directory] [/B] [/H] [pathname [...]]  
  
CIPHER /REKEY [pathname [...]]**Использованная без параметров команда cipher отображает состояние шифрования текущей папки и всех файлов, находящихся в ней.  
  
Параметры командной строки:  
  
**/B** Прервать в случае обнаружения ошибки. По умолчанию CIPHER продолжает выполняться даже при обнаружении ошибок.  
  
**/C** Отображает сведения о зашифрованном файле.   
  
**/D** Расшифровывает указанные файлы или каталоги.   
  
**/E** Шифрует указанные файлы или каталоги. Каталоги будут обозначены, чтобы файлы, добавляемые после этого, шифровались. Зашифрованный файл мог стать зашифрованным во время его изменения в случае, если родительский каталог не зашифрован. Рекомендуется зашифровать файл и родительский каталог.   
  
**/H** Отображает файлы со скрытыми или системными атрибутами. Эти файлы пропускаются по умолчанию.

**/K** Создает новый сертификат и ключ для использования с EFS. Если этот параметр выбран, все остальные параметры будут игнорироваться.  
Примечание. По умолчанию /K создает сертификат и ключ, соответствующие текущей групповой политике. Если требуется ECC, будет создан самоназначаемый сертификат с предоставленным размером ключа.   
  
**/N** Этот параметр работает только с параметром **/U**. Это не позволит обновлять ключи. Данный параметр используется для поиска всех зашифрованных файлов на локальных дисках.   
  
**/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. Если задан параметр SMARTCARD, то ключ восстановления и сертификат записываются на смарт-карту.  
Примечание. По умолчанию /R создает ключ восстановления на 2048 бит RSA и сертификат. Если задан ECC, то после него необходимо указать размер ключа: 256, 384 или 512.   
  
**/P** Создает BLOB-объект политики восстановления, зашифрованный с помощью base64, из предъявленного сертификата. Этот BLOB-объект можно использовать для настройки политики DRA для развертывания MDM.   
  
**/S** Выполняет заданную операцию на указанном каталоге, файлах и подкаталогах в нем.   
  
**/U** Пытается обнаружить все зашифрованные файлы на локальных дисках. Это приведет к обновлению ключа шифрования файлов или ключей восстановления пользователей до текущих в случае их изменения. Данный параметр не работает с другими параметрами, кроме /N.  
  
**/W** Удаляет данные из доступного неиспользуемого дискового пространства на всем томе. Если выбран этот параметр, все остальные будут игнорироваться. Заданный каталог может располагаться в любом месте локального диска. Если это точка или точки подключения к каталогу в другом томе, данные в этом томе будут удалены.   
  
**/X** Создает резервные копии сертификата EFS и ключей и сохраняет их в файл. Если предоставлен файл efsfile, текущий сертификат пользователя, используемый для шифрования файла, будет заархивирован В противном случае будут заархивированы текущие сертификат и ключи EFS пользователя.  
  
**/Y** Отображает текущий отпечаток сертификата EFS на локальном ПКC.  
  
**/ADDUSER** Добавляет пользователя в заданные зашифрованные файлы. Если предоставлен CERTHASH, программа будет искать сертификат с этим хэшем SHA1. Если предоставлен CERTFILE, - извлечет сертификат из файла. Если предоставлен USER, программа будет пытаться найти сертификат пользователя в службах Active Directory Domain Services.   
  
**/FLUSHCACHE** Очищает кэш ключа EFS вызывающего пользователя на указанном сервере. Если имя сервера не указано, программа очистит кэш ключа шифра на локальном компьютере.   
  
**/REKEY** Обновляет указанные зашифрованные файлы для использования текущего ключа EFS.   
  
**/REMOVEUSER** Удаляет пользователя из указанных файлов. CERTHASH должен быть хэшем SHA1 сертификата, который нужно удалить.

**Примеры использования CIPHER**

**cipher /e D:\conf\secutity** - зашифровать подпапку **security** в папке **conf** на диске **D:**  
  
**cipher /e /s:D:\conf** - зашифровать подпапку **conf** и все ее подпапки. В ходе выполнения команды отображается справочная информация:  
  
**Шифрование файлов в D:\conf\  
passwords [OK]  
security [OK]  
Шифрование файлов в D:\conf\passwords\  
far.psw [OK]   
. . .   
  
cipher /s:D:\conf** - отобразить состояние шифрования для папки **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  
. . .   
  
cipher /c /s:D:\conf** - отобразить подробные сведения о зашифрованных файлах. Дополнительно отображается уровень совместимости шифрования для разных версий Windows, сведения о сертификате и ключе шифрования, а также имена пользователей, которые имеют возможность расшифровать данный файл.  
  
**cipher /X** - сохранить резервную копию сертификата EFS и ключей в специальный PFX-файл (PFX сертификат, бинарный формат, при использовании которого в одном зашифрованном файле хранится не только сертификат сервера, но и закрытый ключ) . Имя файла запрашивается перед архивированием. По умолчанию, файл резервной копии сохраняется в домашнем каталоге пользователя и защищается паролем, вводимым пользователем по запросу программы.