**Практическая работа №3**

**Настройка шифрования файлов с помощью EFS.**

**Цель**: изучить настройку шифрования файлов с помощью EFS. **Продолжительность занятия:** 2 часа.

## Задание:

Провести настройку шифрования файлов с помощью EFS.

## Теоретические сведения:

Начиная с Windows XP во всех операционных системах Microsoft существует встроенная технология шифрования данных EFS (Encrypting File System). EFS- шифрование основано на возможностях файловой системы NTFS 5.0 и архитектуре CryptoAPI и предназначено для быстрого шифрования файлов на жестком диске компьютера.

Вкратце опишем схему шифрования EFS. Система EFS использует шифрование с открытым и закрытым ключом. Для шифрования в EFS используется личный и публичный ключи пользователя, которые генерируются при первом использовании пользователем функции шифрования. Данные ключи остаются неизменными все время, пока существует его учетная запись. При шифровании файла EFS случайным образом генерирует уникальный номер, так называемый File Encryption Key (FEK) длиной 128 бит, с помощью которого и шифруются файлы. Ключи FEK зашифрованы master-ключом, который зашифрован ключом пользователей системы, имеющего доступ к файлу. Закрытый ключ пользователя защищается хэшем пароля этого самого пользователя.

Таким образом, можно сделать вывод: вся цепочка EFS шифрования, по сути, жестко завязана на логин и пароль пользователя. Это означает, что защищённость данных в том числе зависит и от стойкости пароля пользователя.

Важно. Данные, зашифрованные с помощью EFS, могут быть расшифрованы только с помощью той же самой учетной записи Windows с тем же паролем, из-под которой было выполнено шифрование. Другие пользователи, в том числе администраторы, расшифровать и открыть эти файлы не смогут. Это означает, что приватные данные останутся в безопасности, даже если [пароль пользователя будет](https://winitpro.ru/index.php/2012/11/09/sbros-parolya-v-windows-8/) [сброшен](https://winitpro.ru/index.php/2012/11/09/sbros-parolya-v-windows-8/) любым способом. Но важно понимать и обратную сторону вопроса. При смене учетной записи или ее пароля (если только он не был изменен непосредственно самим пользователем из своей сессии), выходе из строя или переустановке ОС – зашифрованные данные станут недоступны. Именно поэтому крайне важно экспортировать и хранить в безопасном месте сертификаты шифрования (процедура описана ниже).

Примечание. Начиная с Windows Vista в ОС системах MS поддерживается еще одна технология шифрования – BitLocker. BitLocker в отличии от EFS-шифрования:

используется для шифрования дискового тома целиком

требует наличия аппаратного TPM модуля (в случае его требуется внешнее устройство хранения ключа, например USB флешки или жесткого диска)

Внешне для пользователя работа с зашифрованными с помощью EFS приватными файлами ничем не отличается от работы с обычными файлами – ОС выполняет операции шифрования/дешифрования автоматически (эти функции выполняет драйвер файловой системы).

## Выполнение работы:

В проводник File Explorer выберите каталог или файлы, которые необходимо зашифровать, и, щелкнув ПКМ, перейдите в их свойства (Properties).



На вкладке General в секции атрибутов найдите и нажмите кнопку Advanced.

В появившемся окне поставьте чекбокс Encrypt contents to secure data (Шифровать содержимое для защиты данных).



Нажмите дважды ОК.

В том случае, если выполняется шифрование каталога, система спросит хотите ли вы зашифровать только каталог или каталог и все вложенные элементы. Выберите желаемое действие, после чего окно свойств каталога закроется.

Зашифрованные каталоги и файлы в проводнике Windows отображаются зеленым цветов (напомним, что синим цветов подсвечены объекты, [сжатые на уровне ntfs](https://winitpro.ru/index.php/2012/08/06/nemnogo-pro-szhatye-papki-v-windows/)). Если выбрано шифрование папки со всем содержимым, все новые объекты внутри зашифрованного каталога также шифруются.



Управлять шифрованием/дешифрованием EFS можно из командной строки с помощью утилиты cipher. Например, зашифровать каталог C:\Secret можно так:

cipher /e c:\Secret

Список всех файлов в файловой системе, зашифрованных с помощью сертификата текущего пользователя, можно вывести с помощью команды:

cipher /u /n

Резервное копирование ключа шифрование EFS

После того, как пользователь впервые зашифровал свои данные с помощью EFS, в системном трее появится всплывающее окно, сообщающее о необходимости сохранить ключ шифрования.

Back up your file encryption key. This helps you avoid permanently losing access to you encrypted files.

Щелкнув по сообщению, вы запустите мастер резервного копирования сертификатов и ассоциированных с ними закрытых ключей шифрования EFS.

Если вы случайно закроете окно, или оно не появится, экспортировать сертификаты EFS можно с помощью функции «Manage file encryption certificates» в панели управления пользователями.



Выберите Back up your file encryption certificate and key



Далее запустится мастер экспорта сертификата. Все настройки экспорта можно оставить стандартными (формат Personal Information Exchange — PKCS #12 .PFX)

Затем укажите пароль для защиты сертификата (желательно достаточно сложный).



Осталось указать местоположение, куда необходимо сохранить экспортируемый сертификат (в целях безопасности в дальнейшем его необходимо скопировать на внешний жесткий диск /usb флешку и хранить в безопасном месте).