**Министерство науки и высшего образования Российской Федерации**

**ФГАОУ ВО «Севастопольский государственный университет»**

**Институт информационных технологий и управления в технических процессах**

**Отчёт**

ПО ЛАБОРАТОРНОЙ РАБОТЕ №9

«КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА В ОС WINDOWS»

по дисциплине «Операционные системы»

Выполнил:

студент группы ПИ/б-18-1-о

Николенко Виктория

Проверил:

ст.пр. Шалимова Е.М.

Севастополь

2020

**9.1 Цель работы:** Ознакомление с криптографическими средствами защиты, приобретение практических навыков шифрования файлов и генерации ключей.

**9.2 Порядок выполнения**

9.2.1 Шифрование файла

9.2.2 Шифрование сменных носителей информации

**9.3 Ход работы**

9.3.1 Выберем защищаемый файл. С помощью правой кнопки мыши вызвать контекстное меню и выбрать пункт *Свойства*. На вкладке *Общие* в разделе *Атрибуты* нажать кнопку *Другие.* Откроется окно *Дополнительные атрибуты*. В этом окне в разделе Атрибуты сжатия и шифрования включить *флажок Шифровать* содержимое для защиты данных, нажать ОК.

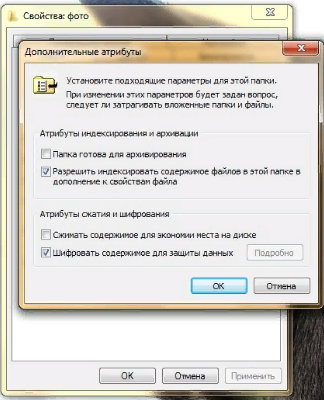


Рисунок 9.1 – Шифрование содержимого для защиты

Для проверки вызовем окно *Панель управления*, нажав на кнопку *Пуск*, открыть раздел *«Параметры папок».* Перейти на вкладку *Вид* и в разделе *Дополнительные параметры* установить флажок *Отображать сжатые или зашифрованные файлы NTFS другим цветом.*

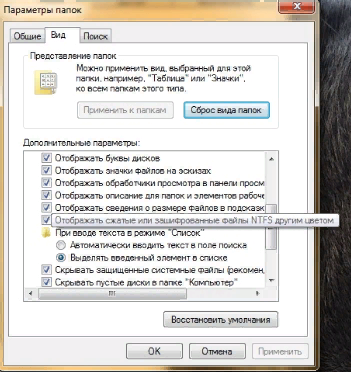


Рисунок 9.2 – Окно «Параметры папок», вкладка «Вид»

Для удобства шифрования и дешифрования файлов включим в контекстном меню соответствующие пункты. Выполняется это путем редактирования реестра. Для вызова утилиты редактирования реестра ***regedit*** в меню *Пуск* в строке Поиск набрать ***regedit,*** В окне программы выполнить двойной щелчок по regedit.exe. Откроется окно редактора. Перейти в раздел ***HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Explorer\Advanced и создать параметр: «EncryptionContextMenu»=dword:00000001»***

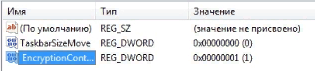


Рисунок 9.3 – Окно «Редактор реестра»

Создание сертификатов ключей. В меню *Пуск* в строке *Поиск* наберём mmc.exe, в окне *Программы* выполним двойной щелчок по ***mmc*** и запустим консоль. В открывшейся консоли нажать CTRL+M или перейдём в меню *Файл > Добавить или удалить оснастку.*

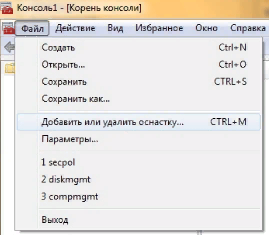
**

Рисунок 9.4 – Добавление оснастки в консоль

В открывшемся окошке в разделе *Доступные оснастки* выберем *Сертификаты* и нажмём кнопку *Добавить*. Открывается окно *Добавление и удаление оснастки*, в котором установим переключатель моей учетной записи пользователя и нажмём *Готово*. Откроется окно *Добавление и удаление оснастки*, в котором нажать ОК

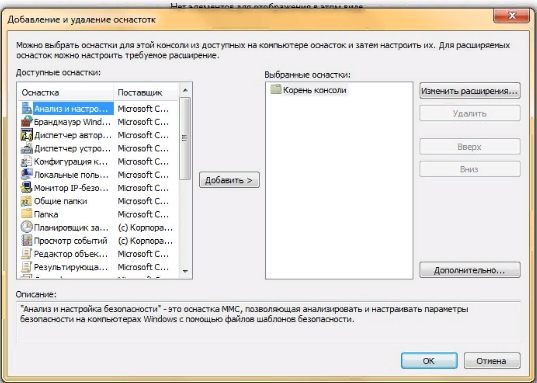


Рисунок 9.5 – Добавление сертификатов

Экспортируем сертификат на рабочий стол, нажав правой кнопкой мыши по *Сертификатам* и выбрав пункт *Экспортировать список* и выберем место экпорта.

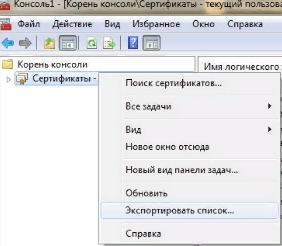


Рисунок 9.6 – Экспортирование сертификата



Рисунок 9.7 – Ярлык сертификата в рабочем столе

9.3.2 Зашифруем сменный носитель информации(диск F). Щелкнув правой кнопкой по значку съемного диска в окне *«Компьютер»*, в контекстном меню выбрать строку *Включить BitLocker*. При выборе опции включения запускается Мастер шифрования диска. На первом шаге мастера Windows введём пароль, который можно использовать для разблокирования диска.

После ввода пароля, Windows генерирует ключ восстановления, сохраним его в файл. И нажмём *Далее*. После сохранения или распечатки ключа восстановления можно шифровать диск. Для этого нажать кнопку *Начать шифрование.*

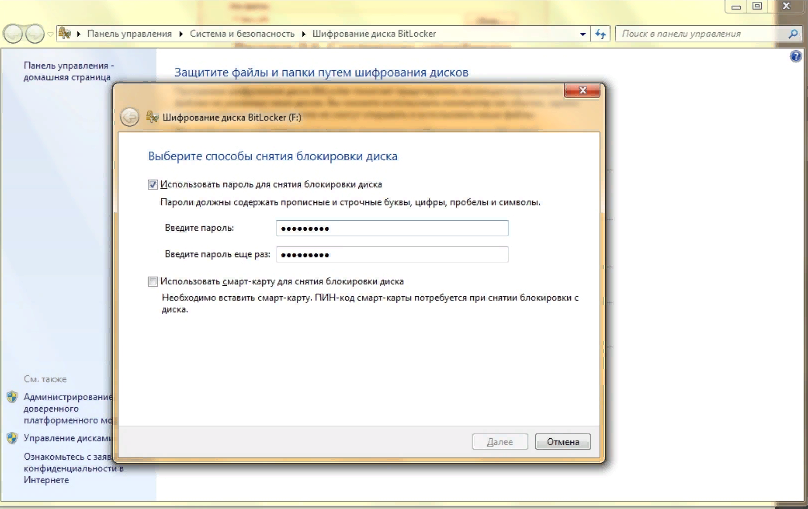


Рисунок 9.8 – Способы блокировки диска

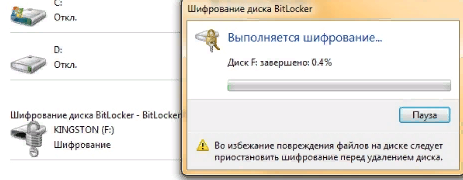


Рисунок 9.9 – Выполнение шифрования

**Вывод**

В ходе лабораторной работы ознакомились с криптографическими средствами защиты, приобрели практических навыки шифрования файлов и генерации ключей.