**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 3

по дисциплине

«Защита электронного технологического документооборота»

«Шифрование данных при хранении»

|  |  |  |
| --- | --- | --- |
| **Выполнил обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г.Е. Груздев |
|  |  |  |
| **Проверил** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | М.Ф. Соломатова |

Санкт-Петербург

2024

**Цель работы**

Проанализировать необходимость шифрования отдельных папок и файлов и оценить возможность снижения рисков информационной безопасности.

**Ход работы**

Изучить работу EFS. Войти под своей учетной записью и с помощью оснастки Certificates запросить сертификат (можно выбрать шаблон User или Basic EFS).

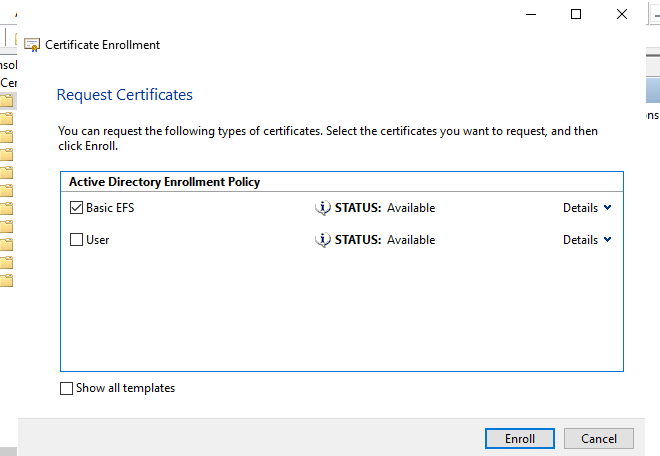


Рисунок 1 – Создание сертификатов

После этого появляется ключевая пара и сертификат открытого ключа. Для шифрования папки в ее свойствах на вкладке General нажать кнопку Advanced, получить доступ к атрибуту, указывающему на шифрование файла, и выполнить шифрование.

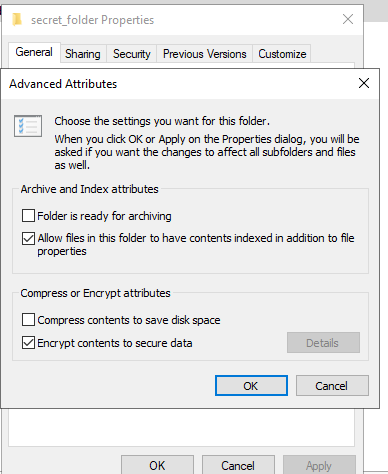


Рисунок 2 – Шифруем данные

Проверить выполнение операций добавления файлов в папку, переименования папки, копирования на другой диск с файловой системой NFTS на том же компьютере, копирования папки на сетевой диск или диск с FAT.

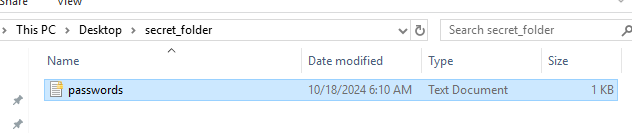


Рисунок 3 – Зашифрованный файл

Войти под учетной записью другого пользователя и попытаться получить доступ к папке и файлам в ней для операций чтения, копирования, переименования и удаления.

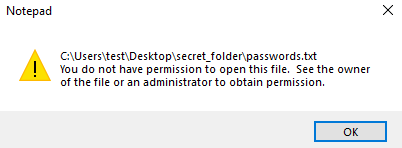


Рисунок 4 – Зашифрованный файл от лица другого пользователя

Снова войти под своей учетной записью. В оснастке Certificates, удалить сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершить сессию пользователя в системе и войти заново. Попробовать открыть зашифрованный файл и выполнить с ним другие операции.

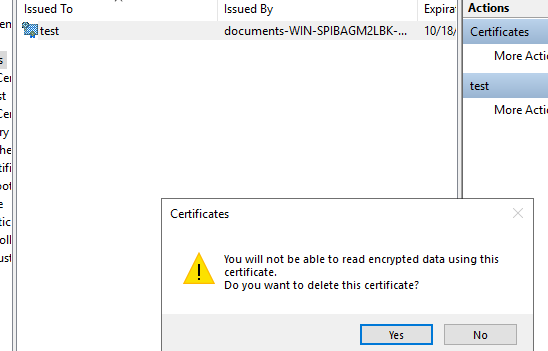


Рисунок 4 – Удаление сертификатов

Войти под учетной записью администратора (агент восстановления по умолчанию). Попробовать расшифровать папку, открыть зашифрованный файл и выполнить с ним другие операции.

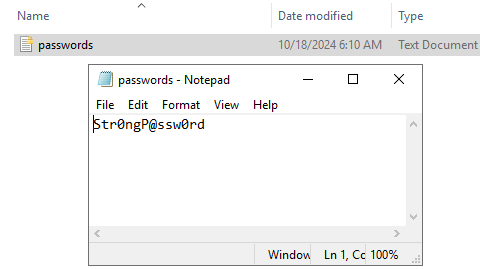


Рисунок 5 – Файл доступен

Отредактировать групповую политику таким образом, чтобы убрать из системы агента восстановления (удалить в политике сертификат). С помощью оснастки Group Policy Management в политике домена найти группу Public Key Policies, пункт Encrypting File System, где указан сертификат агента восстановления. Отредактировать политику (пункт Edit в контекстном меню, далее Policies —> Windows Settings —> Security Settings —> Public Key Policies —> Encrypting File System). Выполнить команду "gpupdate /force" (меню Start—>run—> gpupdate /force) и применить политику.

Повторить все предыдущие действия с папкой под разными учетными записями пользователей. Проанализировать результаты.

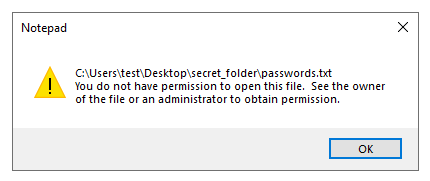


Рисунок 6 – Файл после удаление сертификатов от лица администратора

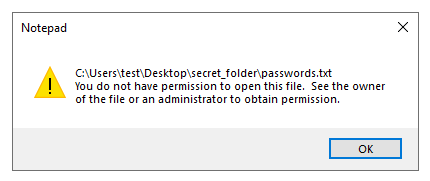


Рисунок 7 – Файл после удаление сертификатов от лица другого пользователя

Вернуть в систему агента восстановления. Для шифрования определить использование нового сертификата, для чего в редакторе политик выбрать политику Encrypting File System, и в контекстном меню выбрать Create Data Recovery Agent. Это приведет к тому, что пользователь Administrator получит новый сертификат и с этого момента сможет восстанавливать шифруемые файлы. Проверить результат.

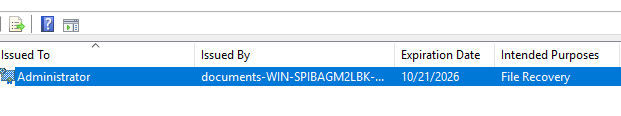


Рисунок 7 – Возвращаем сертификат агента восстановления

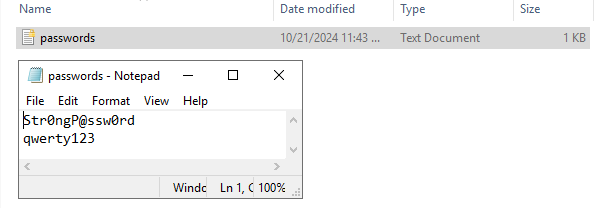


Рисунок 8 – Файл доступен