Министерство образования и науки РФ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Тверской государственный университет»

Математический факультет

Специальность «Компьютерная безопасность»

Кафедра компьютерной безопасности и математических методов управления

**Шифрование в EFS**

курсовая работа по дисциплине

**«Модели безопасности компьютерных систем»**

Автор:

Кокорин Д.А., четвёртый курс, группа М-44

Научный руководитель:

к.ф.-м.н., доц.

Семыкина Н.А.

Тверь 2020

СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc58264450)

[ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ 3](#_Toc58264451)

[Шифрование в EFS 3](#_Toc58264452)

[Описание работы 3](#_Toc58264453)

[Создание политики безопасности операционной системы 5](#_Toc58264454)

[СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 12](#_Toc58264455)

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Шифрование в EFS

Encrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NT (начиная с Windows 2000 и выше), за исключением «домашних» версий (Windows XP Home Edition, Windows Vista Basic, Windows Vista Home Premium, Windows 7 Starter (Home Basic и Premium), Windows 10 Pro, Enterprise и Education издания, Windows Server 2016, Windows Server 2019). Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой NTFS, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам.

Аутентификация пользователя и права доступа к ресурсам, имеющие место в NT, работают, когда операционная система загружена, но при физическом доступе к системе возможно загрузить другую ОС, чтобы обойти эти ограничения. EFS использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре открытый/закрытый ключ для защиты случайно сгенерированного ключа шифрования для каждого файла. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, и защищённость данных зависит от стойкости пароля пользователя.

Описание работы

EFS работает, шифруя каждый файл с помощью алгоритма симметричного шифрования, зависящего от версии операционной системы и настроек (начиная с Windows XP доступна теоретическая возможность использования сторонних библиотек для шифрования данных). При этом используется случайно сгенерированный ключ для каждого файла, называемый File Encryption Key (FEK), выбор симметричного шифрования на данном этапе объясняется его скоростью по отношению к асимметричному шифрованию.

FEK (случайный для каждого файла ключ симметричного шифрования) защищается путём асимметричного шифрования, использующего открытый ключ пользователя, шифрующего файл, и алгоритм RSA (теоретически возможно использование других алгоритмов асимметричного шифрования). Зашифрованный таким образом ключ FEK сохраняется в альтернативном потоке $EFS файловой системы NTFS. Для расшифрования данных драйвер шифрованной файловой системы прозрачно для пользователя расшифровывает FEK, используя закрытый ключ пользователя, а затем и необходимый файл с помощью расшифрованного файлового ключа.

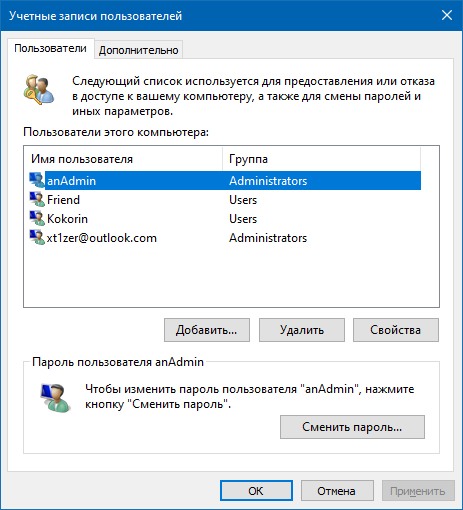
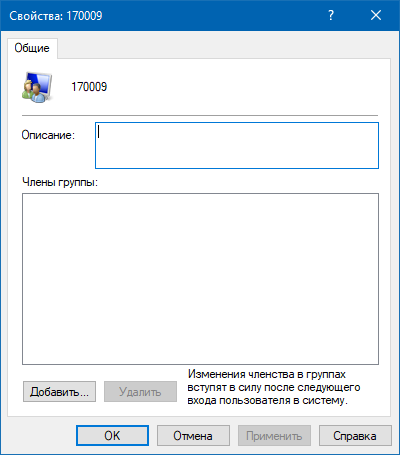
Поскольку шифрование/расшифрование файлов происходит с помощью драйвера файловой системы (по сути, надстройки над NTFS), оно происходит прозрачно для пользователя и приложений. Стоит заметить, что EFS не шифрует файлы, передаваемые по сети, поэтому для защиты передаваемых данных необходимо использовать другие протоколы защиты данных (IPSec или WebDAV).

|  |  |  |
| --- | --- | --- |
| ОС | Алгоритм шифрования по умол. | Алтернатив. алгоритмы |
| Windows 2000 | DESX | Нет |
| Windows XP RTM | DESX | Triple DES |
| Windows XP SP1 | AES | Triple DES, DESX |
| Windows Server 2003 | AES | Triple DES, DESX |
| Windows Vista | AES | Triple DES, DESX |
| Windows Server 2008 | AES | Triple DES, DESX (?) |
| Windows 7  Windows Server 2008 R2 | Смешанный (AES, SHA, ECC) | Triple DES, DESX |

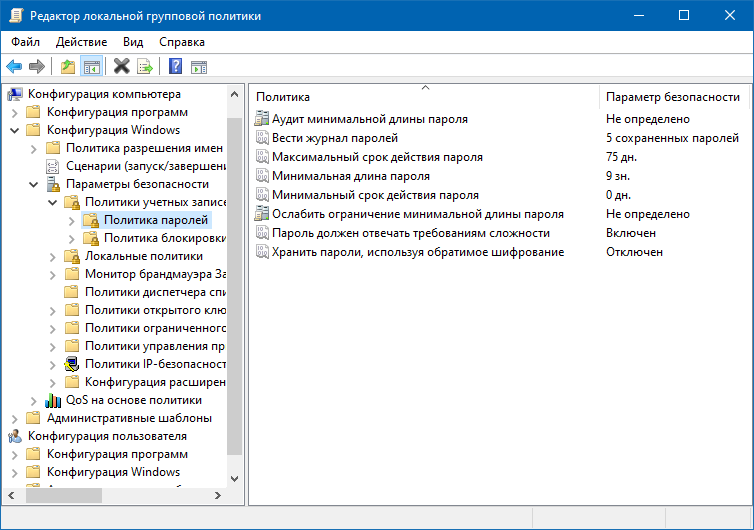
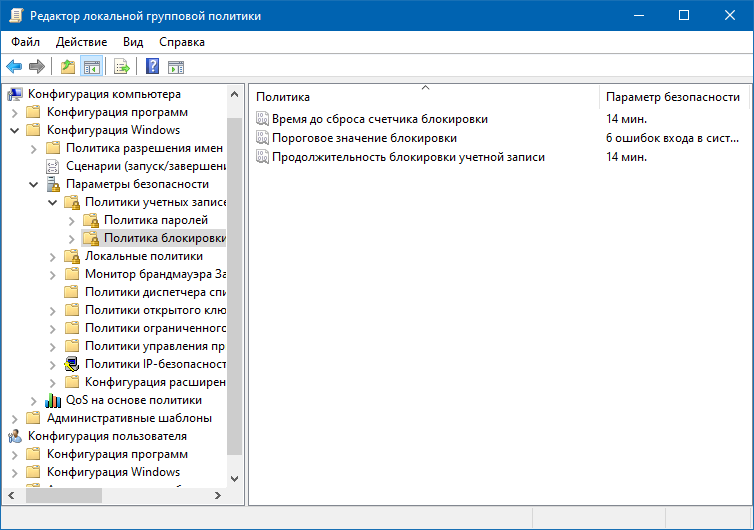
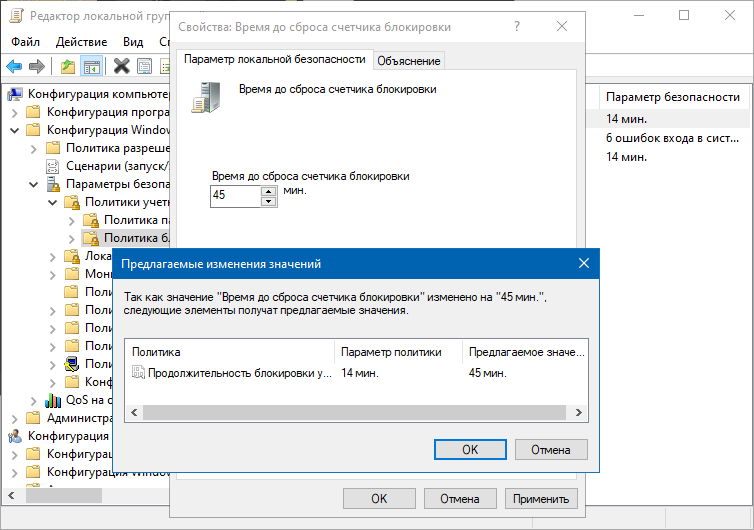
Windows 10 версия 1607 и Windows Server 2016 добавили возможность применения EFS на файловых системах FAT и exFAT.

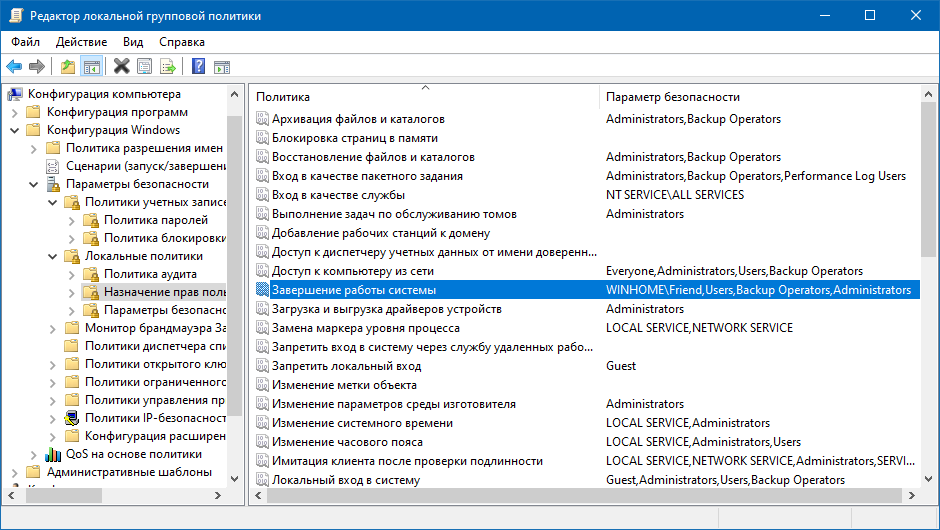
EFS не поддерживается другими операционными системами, кроме Windows изданий Профессиональный и выше для ПК, и Windows Server.

Создание политики безопасности операционной системы

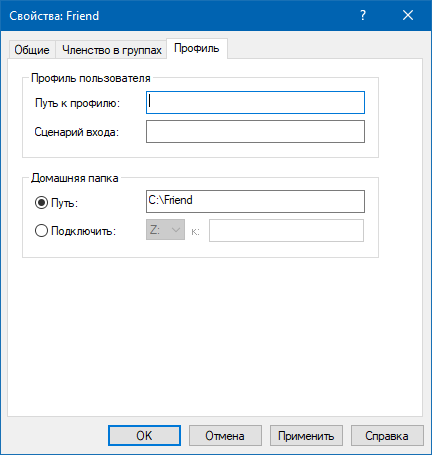
1. Создать учётные записи трёх пользователей: *Администратор*, *Пользователь* (своя фамилия), *Друг*.
2. Создать новую группу пользователей. В качестве имени группы пользователей использовать номер зачётной книжки.
3. Применить к созданной учётной записи *Друг* настройки, указанные в варианте 9:

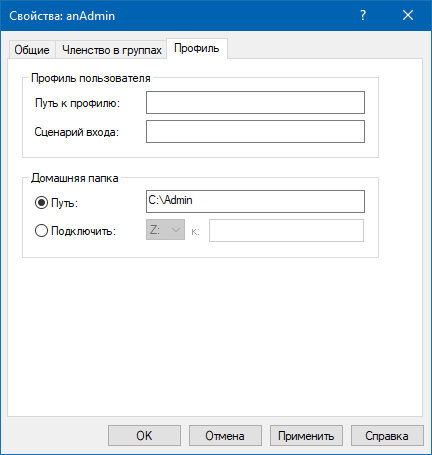
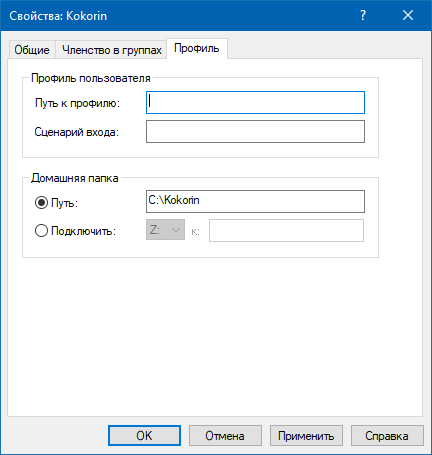
|  |  |
| --- | --- |
| Параметр | Значение |
| Максимальный срок действия пароля | 75 |
| Минимальная длина пароля | 9 |
| Требовать неповторяемости паролей | 5 |
| Пароль должен отвечать требованиям сложности | + |
| Пороговое значение блокировки | 6 |
| Блокировка учётной записи на … мин | 14 |
| Сброс счётчика блокировки через | 45 |
| Завершение работы системы | + |

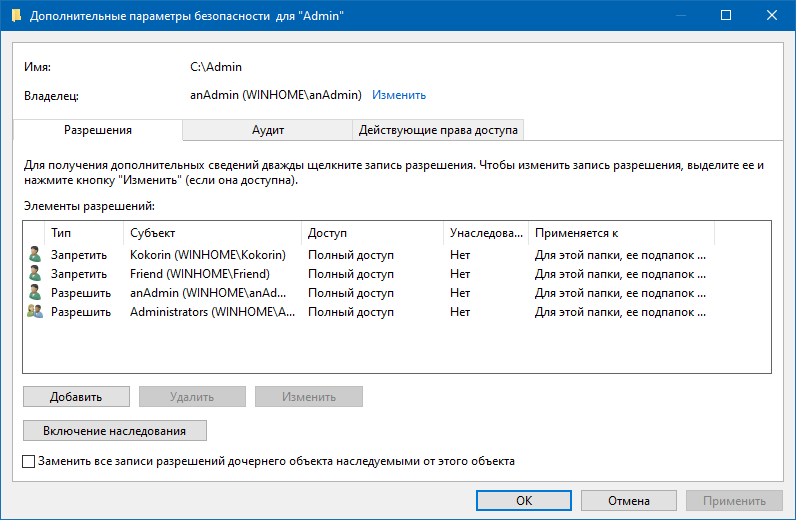
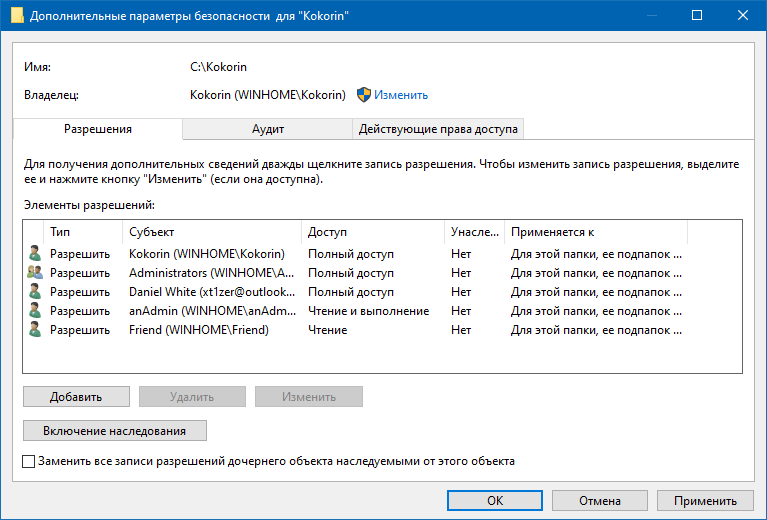
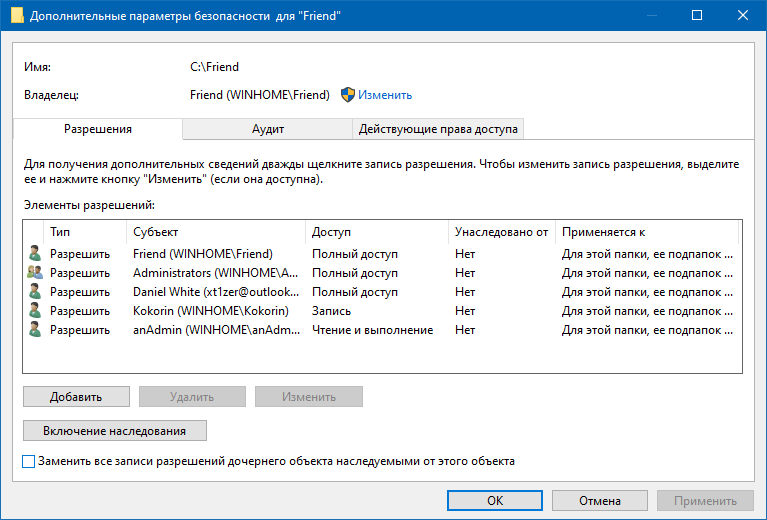
Хочу заметить, что групповая политика не позволяет назначать параметрам «Время до сброса счётчика блокировки» и «Продолжительность блокировки учётной записи» различные значения (см. след. два снимка).

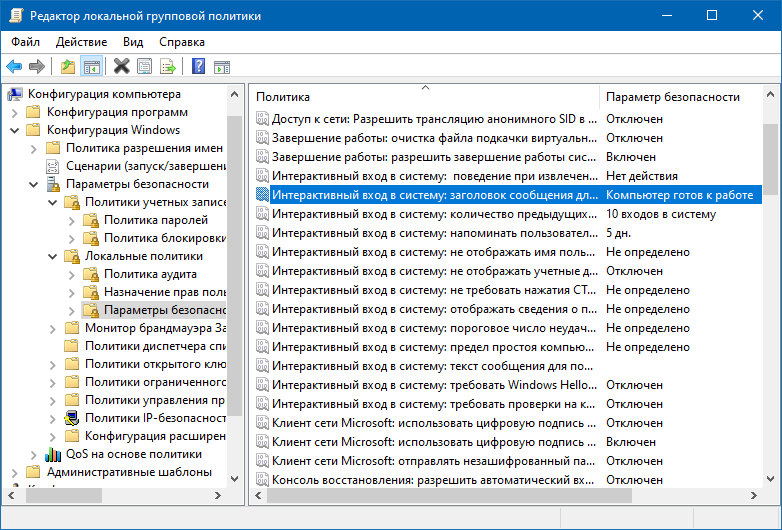
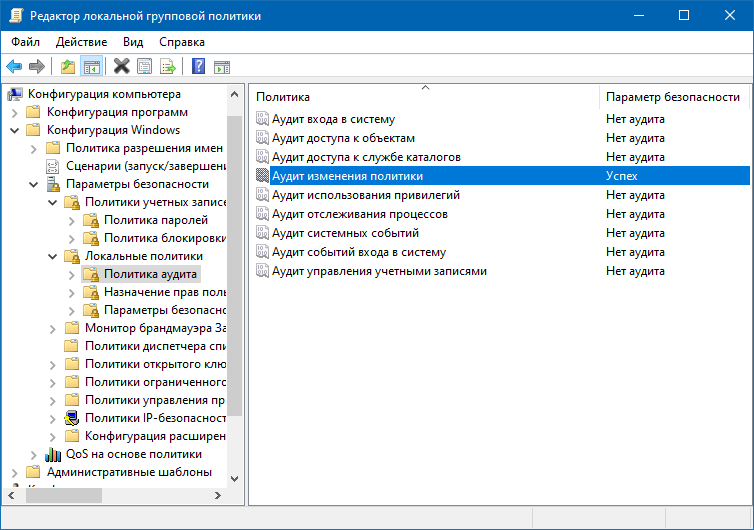
1. *Администратор* компьютера имеет доступ ко всем папкам пользователей на чтение, но не имеет право удалять или изменять файлы. Папка *Администратора* **Disk:\Admin.**

*Пользователь* имеет право записи и чтения в своей папке **Disk:\Собственное имя**, не имеет доступа к папкам *Администратора*, имеет доступ на запись к папке пользователя *Друг*.

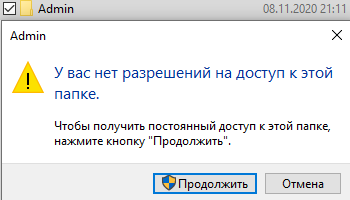
*Друг* имеет право записи и чтения в своей папке **Disk:\Friend**, не имеет доступа к папкам *Администратора*, имеет доступ на чтение к папке *Пользователя*.





1. В качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему» установить текст: «Компьютер готов к работе».
2. С помощью параметров политики аудита установить регистрацию в журнале аудита: изменения политики (успешных попыток).

Пример срабатывания защиты против противоправных действиях пользователя.

*Пользователь* открывает папку *Администратора*:

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. File Encryption – Win32 apps // Microsoft Docs. [2018-2020]. Дата обновления: 31.05.2018. URL: <https://docs.microsoft.com/en-gb/windows/win32/fileio/file-encryption> (дата обращения: 06.12.2020).
2. First Look: New Security Features in Windows Vista // Microsoft TechNet. [2006-2013]. Дата обновления: 05-06.2006. URL: <https://web.archive.org/web/20061110012420/http://www.microsoft.com/technet/technetmag/issues/2006/05/FirstLook/> (дата обращения: 06.12.2020).