**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 5**

на тему «Подсистема аудита и шифрующая файловая система (EFS) в

операционных системах семейства Windows.»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

## **Цель:**

* Изучить защитные механизмы операционной системы Windows, получить навыки практического использования ее средств обеспечения безопасности.

**Ход выполнения работы:**

**Задание 2.2.1.** При выполнении лабораторной работы на компьютерах в учебной лаборатории запустите в программе Oracle VM Virtualbox виртуальную машину Win 7. Войдите в систему под учетной записью администратора. Все действия в п.п. 2.2.1-2.2.6 выполняйте в системе, работающей на виртуальной машине.

Для выполнения лабораторной работы будет использоваться Windows 10 в виртуальной машине Virtual Box. Фото виртуальной машины представлено на рисунке 1.

Изображение выглядит как текст, снимок экрана, Шрифт, Бренд

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 1 – виртуальная машина для лабораторной работы

**Задание 2.2.2.** Создайте учетную запись нового пользователя testUser в оснастке «Управление компьютером» (compmgmt.msc). При создании новой учетной записи задайте произвольный пароль пользователя testUser, запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу ”testGroup” и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске С: папку forTesting. Создайте или скопируйте в эту папку несколько текстовых файлов (\*.txt).

Для создания учетной записи открываем “Управление компьютером” > “Служебные программы” > “Локальные пользователи” > “Пользователи”. Интерфейс, в котором нужно создать пользователя представлен на рисунке 2.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 2 – интерфейс управления компьютером

Нажимаем теперь с помощью ПКМ в центре окна и выбираем “Новый пользователь”. В результате у нас появится такое вот окно, которое представлено на рисунке 3. Сразу же заполним данные, которые требовались для выполнения лабораторной работы. Для пользователя я задал пароль – “1234567890”.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 3 – создание пользователя “testUser”

Теперь перейдем к созданию группы. Для этого слева, как на рисунке 4 выбираем “Группы”.

Изображение выглядит как текст, Шрифт, Значок на компьютере, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4 – интерфейс для переключения окна управления группами

Нажимаем по свободному месту в центральном окне ПКМ, а потом выбираем “Cоздать группу”. Наша задача – дать имя группе, как в условии и добавить пользователя. Конфигурация представлена на рисунке 5.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 5 – создание группы и добавление пользователя

В результате у вас будет такое вот окно, как на рисунке 6 при удачном добавлении пользователя в группу. Остается только нажать на “Cоздать”.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 6 – удачное добавление пользователя в группу

**Задание 2.2.3.** Создайте в разделе HKLM\Software реестра раздел testKey. Запретите пользователю testUser создание новых разделов в этом разделе реестра. Создайте для раздела HKLM\Software\testKey SACL, позволяющий протоколировать отказы при создании новых подразделов, а также успехи при перечислении подразделов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени пользователя testUser запустить regedit.exe и создать раздел в HKLM\Software. Убедитесь, что записи аудита были размещены в журнал безопасности (eventvwr.msc).

Нажимаем комбинацию CTRL + R и вводим туда regedit.exe. Появится окно с редактором реестра. Наша задача перейти по пути Комьютер/HKEY\_LOCAL\_MACHINE/SOFTWARE и там создать раздел testKey. В результате должно получиться то, что представлено на рисунке 7.

Изображение выглядит как текст, программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – создание раздела testKey

Теперь нажимаем правой кнопкой мышки на наш раздел -> разрешения -> дополнительно, выбираем пользователя testUser, а потом нажимает просмотреть, в конце нужно выбрать “Отображение дополнительных разрешений”. Окно с выбором пользователя для управления разрешениями представлено на рисунке 10.

Изображение выглядит как текст, снимок экрана, число, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 – выбор пользователя для управления разрешениями

После этого нам остается выбрать разрешение с названием “Создание подраздела”. В результате выбор разрешения представлен на рисунке 11.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 11 – запрет для пользователя testUser на создание подразделов в разделе testKey реестра

Теперь перейдем к созданию SACL, для этого в окне элемент разрешения нужно выбрать пункты, которые представлены на рисунке 12.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 12 - Создание SACL для отслеживания создания подразделов в разлеле testKey пользователем testUser

Теперь включим аудит на операции, чтобы отследить нашу ошибку. Для этого выбираем также наш реестр, после этого выбираем аудит, как представлено на рисунке 13.



Рисунок 13 – выбор режима для создания аудита

После этого нужно выбрать субъект – testUser - и назначить разрешения, как представлено на рисунке 14.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 14 – параметры для создания аудита

Теперь нужно перейти от имени пользователя testUser в системе и попробовать создать новый подраздел в разделе testKey. В результате должна появится ошибка, которая представлена на рисунке 15.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Операционная система

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – ошибка при создании раздела от лица testUser

Теперь нужно вернуться за нашего администратора и просмотреть системный журнал. Для этого нажимаем CTRL + R и вводим eventvwr.msc, чтобы открылось окно с логами. После этого выбираем пункты по следующему пути: Просмотр событий -> Журналы Windows -> Безопасность. В результате должно выйти то, что представлено на рисунке 16.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – логи от реестра

**Задание 2.2.4. а)** От имени пользователя testUser зашифруйте какой-нибудь файл на диске. Убедитесь, что после этого был создан сертификат пользователя, запустив оснастку certmgr.msc от имени пользователя (раздел Личные). Просмотрите основные параметры сертификата открытого ключа пользователя testUser (срок действия, используемые алгоритмы). Установите доверие к этому сертификату в вашей системе.

Создаем любой текстовый файл от лица testUser, в моем случае это будет – 1.txt. Для выполнения шифрования в командной строке нужно ввести команду cipher /e <Путь к файлу>. В нашем случае получилось то, что представлено на рисунке 17.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 17 – шифрование файла через командную строку

Теперь проверим, что сертификат был удачно создан. Для этого нужно нажать CTRL + R, потом соответственно ввести “certmgr.msc”, у нас откроется окно, которое представлено на рисунке 18. На данном рисунке как раз видно, что был создан новый сертификат.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 18 – сертификат при шифровании

Теперь нужно нажать 2 раза с помощью ЛКМ, у нас откроются характеристики сертификата, которые представлены на рисунке 19.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 19 – параметры сертификата

**Задание 2.2.4. б)** Создайте в папке forTesting новую папку Encrypt. В папке Encrypt создайте или скопируйте в нее текстовый файл. Зашифруйте папку Encrypt и все ее содержимое из меню свойств папки от имени администратора. Попробуйте просмотреть или скопировать какой-нибудь файл этой папки от имени пользователя testUser. Объясните результат. Скопируйте зашифрованный файл в незашифрованную папку (например, forTesting). Убедитесь, что он остался зашифрованным. Добавьте пользователя testUser в список имеющих доступа к файлу пользователей в окне свойств шифрования файла. Повторите попытку получить доступ к файлу от имени пользователя testUser.

Для начала в корне нужно создать директорию forTesting, в ней создать вложенную папку – Encrypt. Для шифрования нужно нажать с помощью ПКМ -> cвойства -> другие -> дополнительно и там выбрать флаг, что нужно шифровать. По умолчанию для Windows 11 не поддерживается. В случае Windows 7 появится такое окно, как представлено ниже на рисунке 20.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 20 – включение шифрования для директории

Если попробовать переместить файл в другое место, то он также останется зашифрованным. Попробуем теперь выдать все разрешения на просмотр директории, как на рисунке 21.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 21 – разрешение на шифрование директории

Если попробуем теперь просмотреть, то все будет удачно, как на рисунке 22.

Изображение выглядит как текст, компьютер, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 22 – удачная попытка просмотра файла

**Задание 2.2.4. в)** Создайте учетную запись нового пользователя agentUser, сделайте его членом группы Администраторы. Определите для пользователя agentUser роль агента восстановления EFS. Создайте в папке forTesting новый текстовый файл с произвольным содержимым. Зашифруйте этот файл от имени пользователя testUser. Убедитесь в окне подробностей шифрования файла, что пользователь agentUser является агентом восстановления для данного файла. Попробуйте прочитать содержимое файла от имени администратора и от имени пользователя agentUser. Объясните результат.

Через управление компьютером создаем нового пользователя. Важно его создать от имени администратора системы, чтобы можно было сразу добавить в группу администраторов. На рисунке 23 представлен интерфейс для создания нового пользователя.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 23 – создание нового пользователя

Теперь создадим сертификаты для агентов восстановления. Для этого в cmd надо выполнить команду – cipher /p:<название сертификата>. В нашем случае получилось то, что представлено на рисунке 24.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 24 – создание сертификатов для агентов восстановления

Нажмите с помощью ЛКМ два раза на сертификат и у вас откроется окно для создания мастера агента восстановления. Если же так не открывается, то данные действия нужно выполнять через Параметры системы.

Изображение выглядит как текст, программное обеспечение, веб-страница, Веб-сайт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 24 – создание агента для восстановления

**Задание 2.2.4. г)** Зашифруйте все текстовые файлы папки forTesting с использованием консольной команды шифрования cipher от имени пользователя testUser.

Теперь выберем файл для шифрования, в нашем случае появится предупреждение о том, что мы собираемся шифровать файл нашим сертификатом, как представлено на рисунке 25.

Изображение выглядит как текст, программное обеспечение, веб-страница, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 25 – предупреждение о шифровании

**Контрольные вопросы**

1. Какие события подлежат аудиту в ОС Windows?

Важный элемент политики безопасности - аудит событий в системе. ОС Windows ведет аудит событий по следующим категориям, которые представлены ниже.

Аудит событий входа в систему: аудит попыток пользователя войти в систему с другого компьютера или выйти из нее, при условии, что этот компьютер используется для проверки подлинности учетной записи.

Аудит управления учетными записями:аудит событий, связанных с управлением учетными записями на компьютере: создание, изменение или удаление учетной записи пользователя или группы; переименование, отключение или включение учетной записи пользователя; задание или изменение пароля.

Аудит доступа к службе каталогов:аудит событий доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

Аудит входа в систему:аудит попыток пользователя войти в систему с компьютера или выйти из нее.

Аудит доступа к объектам:аудит событий доступа пользователя к объекту - например, к файлу, папке, разделу реестра, принтеру и т. п., - для которого задана собственная системная таблица управления доступом (SACL).

Аудит изменения политики:аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит использования привилегий:аудит попыток пользователя воспользоваться предоставленным ему правом.

Аудит отслеживания процессов:аудит таких событий, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Аудит системных событий: аудит событий перезагрузки или отключения компьютера, а также событий, влияющих на системную безопасность или на журнал безопасности

2. Какие события регистрируются в журнале «Аудит изменения политики»?

Аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

3. Каким образом шифруются файлы в файловой системе EFS?

Процесс шифрования представлен на рисунке ниже.

Изображение выглядит как текст, снимок экрана, диаграмма, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

4. Что такое FEK, DDF, DRF?

FEK (File Encryption Key) - случайно сгенерированный симметричный ключ, который используется для непосредственного шифрования файла. Для каждого файла создается свой FEK.

DDF (Data Decryption Field) - поле в метаданных файла, которое содержит FEK, зашифрованный открытым ключом пользователя.

DRF (Data Recovery Field) - поле в метаданных файла, которое содержит FEK, зашифрованный открытым ключом агента восстановления.

5. Какие алгоритмы шифрования используются в EFS?

В разных версиях Windows используются различные алгоритмы:

* Windows 2000/XP: DESX (по умолчанию) или 3DES
* Windows Server 2003/Windows XP: AES-256, 3DES или DESX
* Windows Vista/7/8/10/11: AES-256 с длиной ключа 256 бит (по умолчанию)
* Windows Server 2008/R2/2012/2016/2019/2022: AES-256

6. Какие функции выполняют агенты восстановления в ОС Windows?

Агенты восстановления выполняют следующие функции:

* Восстановление доступа к зашифрованным данным при утере пользовательского сертификата
* Дешифрование файлов при увольнении сотрудника
* Обеспечение соответствия политикам безопасности организации
* Резервное копирование ключей шифрования

7. Как зашифровать файл, используя систему EFS (приведите все возможные варианты)?

Можно через проводник Windows:

1. Щелкните правой кнопкой мыши на файле/папке
2. Выберите "Свойства" → "Дополнительно"
3. Установите флажок "Шифровать содержимое для защиты данных"
4. Нажмите "ОК" и примените изменения