**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 № 4**

на тему «Управление правами доступа 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 концептуальную модель безопасности операционных систем семейства 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

Теперь по условию задания остается в корне диска C:\ cоздать директорию ForTesting. Результат представлен на рисунке 7.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 7 – содержимое директории forTesting

**Задание 2.2.3.** С помощью команды runas запустите сеанс командной строки (cmd.exe) от имени вновь созданного пользователя. Командой whoami посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя.

Для запуска сеанса командной строки от нашего нового пользователя нужно выполнить несколько действий. Нажмите Win + R, а потом вставьте команду – “runas /user:testUser cmd”. Вставьте команду и выполните, после чего вас попросят ввести пароль. Вызов и открытие консоли представлено на рисунке 8.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 – открытие сессии в терминале пользователя testUser

Теперь посмотрим с помощью команды “whomai /all” SID пользователя и всех его групп, а также его в привилегии. Результат представлен на рисунке 9.

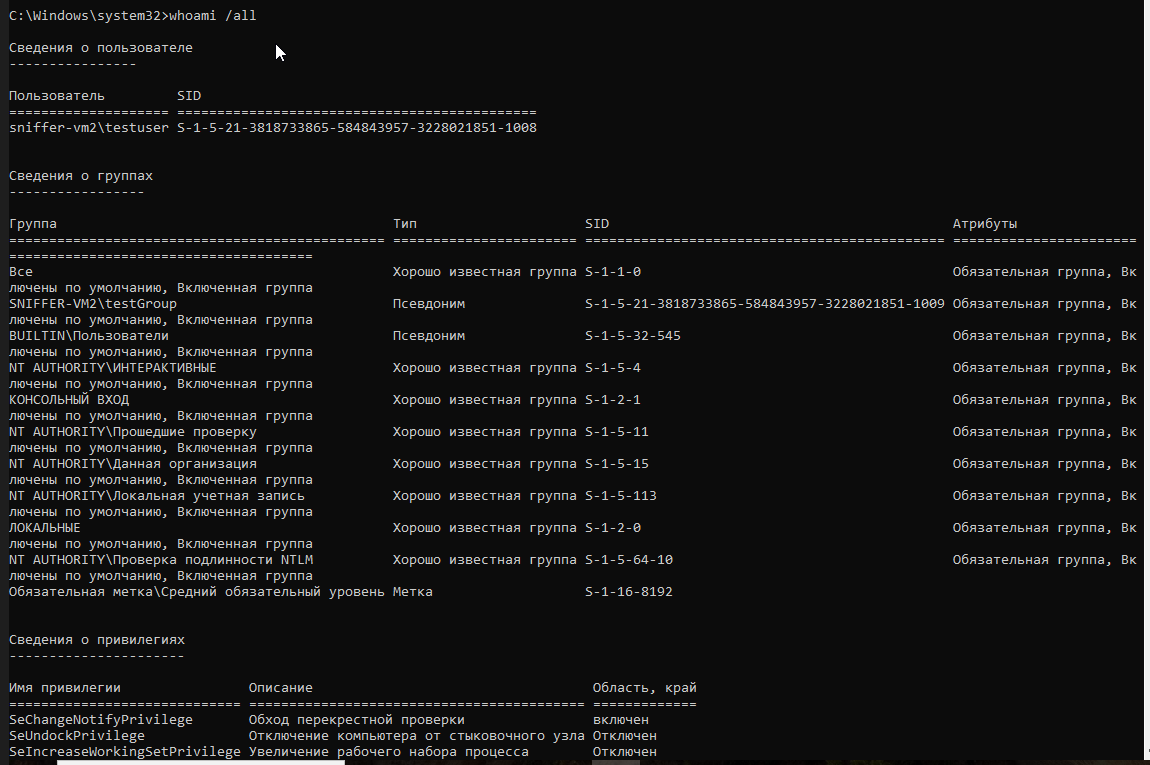


Рисунок 9 – просмотр результата whoami

**Задание 2.2.4.** Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен 14 SID S-1-5-21-…………-………-…………-1002. (Используйте ключ реестра HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList).

У моего пользователя получился такой вот SID. На рисунке 10 представлен вывод с терминала командой whoami.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 – SID пользователя в системе

Теперь просмотрим то, что получилось в реестре. Для этого в поиске вводим Редактор Реестра. Потом переходим по такому вот пути: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Там у вас откроется список профилей, после этого у вас есть возможность просмотреть информацию о пользователе. Результат представлен на рисунке 11.

Изображение выглядит как текст, снимок экрана, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 11 – содержимое реестра для пользователя testUser

**Задание 2.2.5.** Командой whoami определите перечень текущих привилегий пользователя testUser. В сеансе командной строки пользователя попробуйте изменить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» раздела Локальные политики -> Назначение прав пользователя. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. Попробуйте изменить системное время командой time. Убедитесь, что привилегия «Завершение работы системы» (SeShutdown - Privilege) предоставлена пользователю testUser . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой shutdown -s. Добавть ему привилегию «Принудительное удаленное завершение» (SeRemoteShutdownPrivilege). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой shutdown -a).

Для просмотра привилегий воспользуемся командой “whoami /prev”, в результате у нас выйдет то, что представлено на рисунке 12.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 12 – просмотр привилегий для пользователя testUser

Теперь попробуем поменять время на 15:45:00. Для этого воспользуемся командой “time 15:45:00”. На рисунке 13 представлено, что у пользователя нет права поменять время, выдает ошибку доступа.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 13 – попытка смены времени для пользователя

Теперь выдадим пользователю доступ на изменение системного времени. Для этого открываем “Локальные политики безопасности” через поиск Windows. После этого выполняем: Локальные политики > Назначение прав пользователя > Изменение системного времени. В результате у вас должно получиться то, что представлено на рисунке 14.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 14 – добавление возможности управлять временем для пользователя testUser

Теперь у пользователя testUser есть возможность менять время. Результат представлен на рисунке 15.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – удачное изменение времени пользователем testUser

При создании пользователя testUser он был удалён из группы Пользователи, но т.к. в эту группу входят «Прошедшие проверку» (в это время пользователь testUser прошёл проверку при запуске командной строки от его имени), привилегия SeShutdownPrivilege выдаётся ему автоматически. Используемая команда – “shutdown -s”.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – выключение компьютера от имени пользователя

**Задание 2.2.6.** Ознакомьтесь со справкой по консольной команде icacls. Используя эту команду, просмотрите разрешения на папку c:\forTesting. Объясните все обозначения в описаниях прав пользователей и групп в выдаче команды.

Для выполнения задания нужно использовать команду “icacls C:\forTesting”. Результат представлен на рисунке 17.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 17 – просмотр разрешения на директорию icacls

(OI) -  Object inherit – права наследуются на нижестоящие объекты

(CI) - Container inherit – наследование каталога

(F) – Full control– полный доступ к папке

(I) — Inherit   права наследованы с вышестоящего каталога

(IO) — inherit only

(NP) — don’t propagate inherit

(I) — Permission inherited from parent container

D — право удаления

F — полный доступ

N — нет доступа

M — доступ на изменение

RX — доступ на чтение и запуск

R — доступ только на чтение

W — доступ только на запись

**Задание 2.2.6.** **Пункт а).** Разрешите пользователю testUser запись в папку forTesting, но запретите запись для группы testGroup. Попробуйте записать файлы или папки в forTesting от имени пользователя testUser. Объясните результат. Посмотрите эффективные разрешения пользователя testUser к папке forTesting в окне свойств папки.

Для выдачи прав записи для пользователя нужно воспользоваться 2 командами. “icacls "C:\forTesting" /grant testUser:(W)” – разрешить пользователю записывать в файл, “icacls "C:\path\forTesting" /deny testGroup:(W)” – запретить группе записывать в файл. В результате вышло то, что представлено на рисунке 18.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 18 – выдача прав на запись в файл

Теперь попробуем записать в файл, в результате произойдет такая ошибка, которая представлена на рисунке 19. Такое происходит по той причине, потому что пользователь находится в группе, которой запрещено записывать данные в текущую директорию.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 19 – запрет на добавление файлов в директорию forTesting

**Задание 2.2.6. Пункт б).** Используя стандартное окно свойств папки, задайте для пользователя testUser такие права доступа к папке, чтобы он мог записывать информацию в папку forTesting, но не мог просматривать ее содержимое. Проверьте, что папка forTesting является теперь для пользователя testUser “слепой”, запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки.

Зададим разрешение на директорию. Для этого через ПКМ нажимаем на директорию > Свойства > Безопасность > Дополнительно. Предоставленная конфигурация на рисунке 20 выполняет полностью условие задания. Также на рисунке предоставлен результат попытки просмотра содержимого директории. Через проводник и терминал файл у нас не будет найден, что говорит о корректности настройки.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 20 – попытка чтения директории за разных пользователей

**Задание 2.2.6. Пункт в).** Для вложенной папки forTesting\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка forTesting\Docs перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

Создайте в папке forTesting папку Docs. Для отключения наследования делаем следующие действия: ПКМ по папке > свойства > Безопасность > Дополнительно > Отключение наследования. Конфигурация для выполнения задания представлена на рисунке 21.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 21 – конфигурация прав директорий для выполнения задания

Попробуем теперь через проводник просмотреть содержимое директории. На рисунке 22 представлен удачный просмотр содержимого директории.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 21 - успешная попытка чтения папки C:\forTesting\Doc от имени пользователя testUser

Попробуем теперь создать файлы и директории. В нашем случае получилось все создать. Результат представлен на рисунке 23.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 23 - успешное создание и чтение папок и файлов в папке Docs

**Задание 2.2.6. Пункт г).** Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду icacls запретите этому пользователю доступ к файлам с расширением txt в папке forTesting. Убедитесь в недоступности файлов для пользователя.

Опять-таки через безопасность в свойствах нужно включить разрешение для чтения директории forTesting для пользователя testUser. Теперь воспользуемся командой “icacls “C:\forTesting” /remove:d testUser”. В результате после выполнения команды должно выйти то, что представлено на рисунке 24.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 24 – конфигурация для выполнения задания

Теперь попробуем открыть любой txt файл, у нас вылетит ошибка, которая представлена на рисунке 25.

Изображение выглядит как текст, снимок экрана, Операционная система, мультимедиа

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 25 – отказ в доступе при попытке открыть txt файл

**Задание 2.2.6. Пункт д).** Командой icacls запретите пользователю все права на доступ к папке forTesting и разрешите полный доступ к вложенной папке forTesting\Docs. Убедитесь в доступности папки forTesting\Docs для пользователя. Удалите у пользователя testUser привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. Объясните результат, записать в выводы.

Для полного запрета к директории forTesting воспользуйтесь командой: “icacls "C:\forTesting" /deny testUser:(F)”. После выполнения первой команды у вас получится то, что представлено на рисунке 26.

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 26 – полная блокировка директории forTesting

Для разрешения полного доступа к вложенной папке Docs воспользуйтесь командой: “icacls "C:\forTesting\Docs" /grant testUser:(F)”. В результате должно выйти то, что представлено на рисунке 27.

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 27 – полный доступ к подпапке

Попробуем теперь прочитать подпапку. Результат представлен на рисунке 28.

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 28 – чтение данных из подпапки

Теперь удалим у пользователя привилегию SeChangeNotifyPrivilege. Перейдите в Локальные политики -> Назначение прав пользователя. В правой панели найдите политику "Обход перекрестной проверки" (или "Bypass traverse checking"). Нажмите пару раз и выключите данный параметр. В результате у вас должно получиться то, что представлено на рисунке 29.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 29 – недоступность для просмотра директории

**Задание 2.2.6. Пункт е).** Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

Для выполнения данного пункта создадим директорию newFolder в корне диска C. Теперь сделаем наследование от родительской директории, чтобы получить все права такие же. Для выполнения данного действия воспользуйтесь командой: “icacls «C:\newFolder» /inheritance:r”. В результате должно получиться то, что представлено на рисунке 30.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 30 – выполнение команды для определения прав

Попробуем теперь открыть директорию от имени пользователя testUser. На рисунке 31 видим, что нет разрешений на доступ к данной директории.

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 31 – запрет на доступ к данной директории

**Задание 2.2.6. Пункт ж).** С использованием команды whoami проверьте уровень целостности для пользователя testUser и администратора (учетная запись ВПИ). Запустите какое-нибудь приложение (калькулятор, блокнот) от имени testUser и администратора. С использованием утилиты ProcessExplorer (можно найти в папке c:\Utils на виртуальной машине) проверьте уровень целостности запущенных приложений. Объясните разницу. Верните пользователю testUser права на полный доступ к папке forTesting. От имени администратора создайте в папке forTesting текстовый файл someText.txt. Измените уровень целостности этого файла до высокого с использованием команды icacls. Запустите блокнот от имени пользователя testUser, откройте в нём файл someText.txt, измените содержимое файла и попробуйте сохранить изменения. Объясните причину отказа в доступе. Как можно предоставить пользователю testUset доступ к файлу?

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 32 - пользователь testUser обладает средним уровнем целостности

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 33 - пользователь sergey-vm1 обладает средним обязательным уровнем целостности

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 34 - пользователь Администратор обладает Высоким уровнем целостности

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 35 - создание файла new.txt от имени Администратора

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 36 - изменение уровня целостности файла до высокого, отказ в доступе к файлу new.txt от имени пользователя testUser

Вывод. В данной лабораторной работе была изучена концептуальная модель безопасности операционных систем семейства Windows, а также получены навыки практического использования ее средств обеспечения безопасности.

**Задание 2.2.7.** После окончания работы восстановить исходное состояние системы: удалить созданные папки и файлы, разделы реестра, удалить учетную запись созданного пользователя и его группы.

**Контрольные вопросы**

1. К какому классу безопасности относится ОС Windows по различным критериям оценки?

Так, по классификации «Оранжевой книги» ОС Windows NT 4 еще в 1999 году получила класс безопасности C2, по стандарту ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий) клиентские и серверные версии от Windows 2000 до Windows 10, от Windows Server 2008 до Windows Server 2013 получили уровень безопасности EAL4+, а операционные системы Windows 8, Windows Server 2012 Standard соответствуют требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) по 5 классу защищенности.

2. Каким образом пользователи идентифицируются в ОС Windows?

Все действующие в системе объекты (пользователи, группы, локальные компьютеры, домены) идентифицируются в Windows не по именам, уникальность которых не всегда удается достичь, а по идентификаторам защиты (Security

Identifiers, SID). SID представляет собой числовое значение переменной длины:

S - R - I - SO - S1 - ... - Sn - RID

S - неизменный идентификатор строкового представления SID;

R - уровень ревизии (версия). На сегодня 1.

I - (identifier-authority) идентификатор полномочий

Sn - 32-битные коды (количеством 0 и более) субагентов, которым было передано право выдать SID.

Остальные подчиненные полномочия идентификатора совместно обозначают домен или компьютер, который издал идентификатор SID.

RID - 32-битный относительный идентификатор. Он является идентификатором уникального объекта безопасности в области, для которой был определен SID.

3. Что такое списки DACL и SACL?

DACL (discretionary access control list) — это список, который определяет разрешения на доступ для пользователей и групп к объектам.

SACL (System Access Control List) — список управления доступом к объектам Microsoft Windows, используемый для аудита доступа к объекту.

4. Перечислите, каким образом можно запустить процесс от имени другого пользователя.

Существует несколько способов запустить процесс от имени другого пользователя в Windows. Вот некоторые из них:

Через контекстное меню Windows. Для этого нужно: — Удерживая клавишу Shift, нажать правой кнопкой мыши по ярлыку или исполняемому файлу программы.

— В контекстном меню выбрать пункт «Запуск от имени другого пользователя».

— Ввести имя другого пользователя и соответствующий этой учётной записи пароль.

В командной строке. Для этого нужно: — Открыть командную строку.

— Ввести команду: runas /user:ИМЯ\_пользователя «Полный путь к файлу программы и параметры запуска при необходимости».

— Ввести пароль выбранной учётной записи пользователя, если он будет запрошен.

5. Как происходит проверка прав доступа пользователя к ресурсам в ОС Windows?

Авторизация Windows основана на сопоставлении маркера доступа субъекта с дескриптором безопасности объекта. Управляя свойствами объекта, администраторы могут устанавливать разрешения, назначать право владения и отслеживать доступ пользователей.

Список управления доступом содержит набор элементов (Access Control Entries, ACE). В DACL каждый ACE состоит из четырех частей: в первой указываются пользователи или группы, к которым относится данная запись, во второй - права доступа, а третья информирует о том, предоставляются эти права или отбираются. Четвертая часть представляет собой набор флагов, определяющих, как данная запись будет наследоваться вложенными объектами (актуально, например, для папок файловой системы, разделов реестра). Если список ACE в DACL пуст, к нему нет доступа ни у одного пользователя (только у владельца на изменение DACL). Если отсутствует сам DACL в SD объекта - полный доступ к нему имеют все пользователи. Если какой-либо поток запросил доступ к объекту, подсистема SRM (Security reference Monitor, монитор состояния защиты) осуществляет проверку прав пользователя, запустившего поток, на данный объект, просматривая его список DACL. Проверка осуществляется до появления разрешающих прав на все запрошенные операции. Если встретится запрещающее правило хотя бы на одну запрошенную операцию, доступ не будет предоставлен.

6. Что такое маркер безопасности, и какова его роль в модели безопасности Windows?

После аутентификации пользователя процессом Winlogon, все процессы, запущенные от имени этого пользователя будут идентифицироваться специальным объектом, называемым маркером доступа (access token). Если процесс пользователя запускает дочерний процесс, то его маркер наследуются, поэтому маркер доступа олицетворяет пользователя для системы в каждом запущенном от его имени процессе.

Маркер доступа содержит идентификатор доступа самого пользователя и всех групп, в которые он включен. В маркер включен также DACL по умолчанию - первоначальный список прав доступа, который присоединяется к создаваемым пользователем объектам.

7. Как с использованием команды icacls добавить права на запись для всех файлов заданной папки?

Icacls [путь к файлу или папке] /grant:r [имя пользователя]:W

8. Что такое уровень целостности? Как он влияет на права доступа субъектов к объектам ОС? Как можно узнать и задать уровень целостности для объектов и субъектов?

Базовым понятием WIC является уровень целостности (integrity level) объекта. WIC присваивает контролируемым объектам один из шести доступных уровней целостности: - Untrusted — анонимные процессы автоматически попадают в эту категорию. - Low — стандартный уровень при работе с Интернетом. Если браузер Internet Explorer запущен в защищенном режиме, все файлы и процессы, ассоциированные с ним, назначаются в эту категорию. Некоторые папки, такие как, например, Temporary Internet Folder, также по умолчанию наделяются Низким уровнем доверия. - Medium — в данном контексте работает большинство объектов. Ординарные пользователи получают Средний уровень, всем объектам присваивается данный уровень доступа, если не указан какой-либо иной. - High — уровень, ассоциированный в системе с Администраторами. Объекты Высокого уровня недоступны обычным пользователям. - System — уровень для работы ядра операционной системы и его служб. - Installer — вершина в иерархии уровней WIC. Его объекты могут изменять и удалять файлы всех предыдущих уровней. Контроль по уровням целостности при доступе к объекту также 12 осуществляется на основе правил ACE. Но это специализированные ACE, которые начиная с Windows Vista хранятся в списке SACL дескриптора безопасности объекта наряду с правилами аудита. Уровень целостности пользователя (процесса, выполняющегося от его имени) хранится в его токене безопасности.

Для изменения уровня целостности объектов можно использовать следующие инструменты:

- уже рассмотренную команду icacls с ключом /setintegitylevel. Например, вот так можно присвоить файлу низкий (l) уровень целостности:

icacls f:\temp /setintegritylevel l

- используя специальные утилиты Chml ("change mandatory label" ) для изменения уровня целостности файлов и папок, и Regil ("Registry integrity levels") для работы с уровнями целостности ключей реестра.

Изменить уровень целостности процесса можно, например, запустив его утилитой psexec .exe с соответствующим ключом. Вот как можно запустить блокнот с высоким уровнем целостности: psexec -h notepad.exe

Очевидно, что изменять уровень целостности запускаемых процессов потенциально небезопасная операция, поэтом ее могут запускать только процессы, у которых в маркере доступа установлена привилегия SeRelabelPrivilege.