

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 «Концептуальная модель безопасности ОС семейства Windows.»

Выполнил обучающийся гр. ВКБ42

Михайлов А.С.

Проверил:

Доцент Скляров А.В.

Ассистент Кацай А.М.

Ростов-на-Дону

2024

Цель работы: изучить концептуальную модель безопасности операционных

систем семейства Windows, получить навыки практического использования ее

средств обеспечения безопасности.

Ход работы:

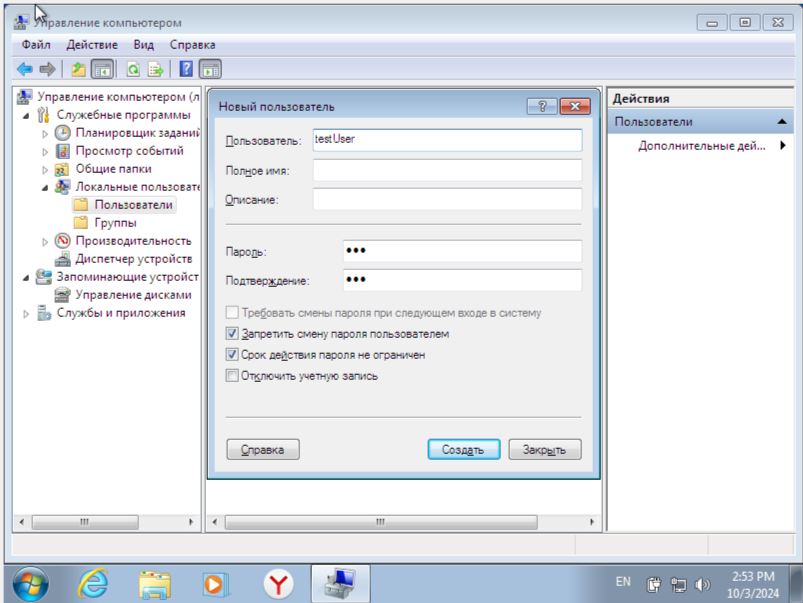


Рисунок 1 – Создание пользователя

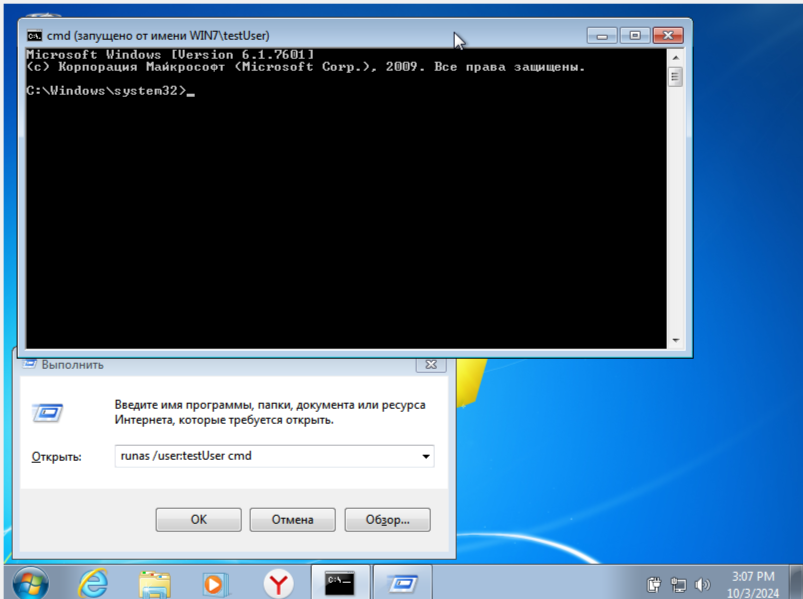


Рисунок 2 – Запуск командной строки с другого пользователя

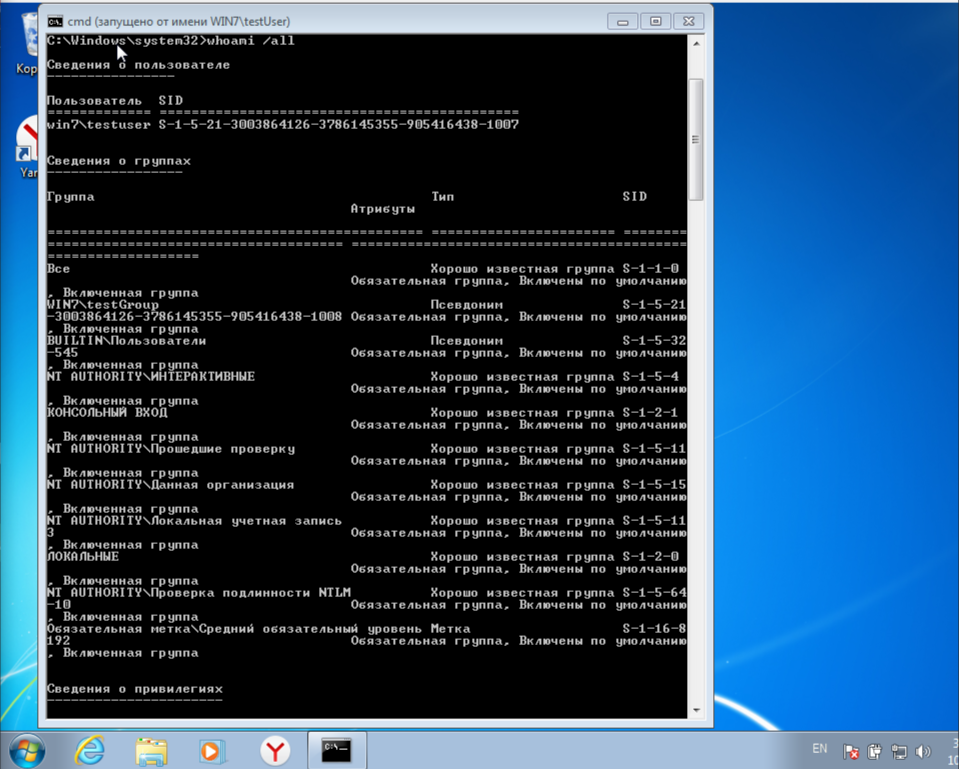


Рисунок 3 – Результат команды Whoami /all

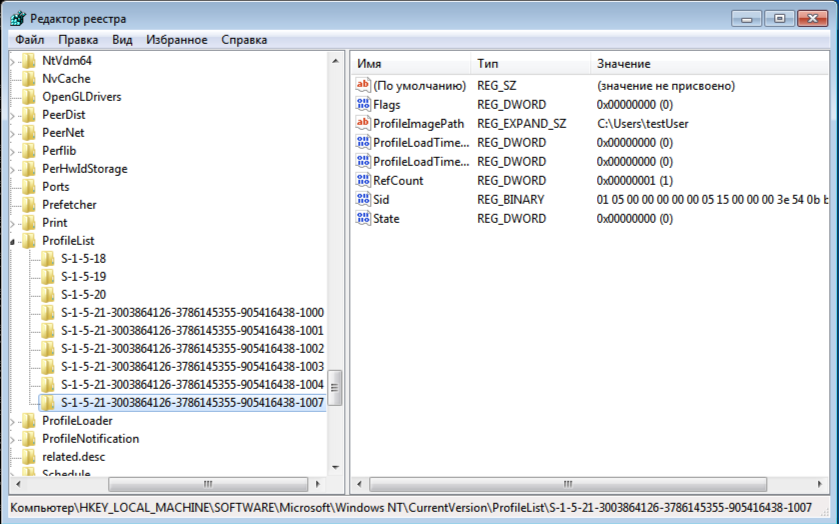


Рисунок 4 – SID пользователя в реестре

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

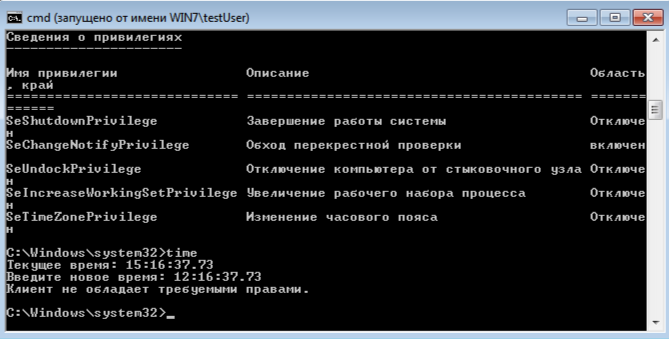


Рисунок 5 - Результат изменения времени

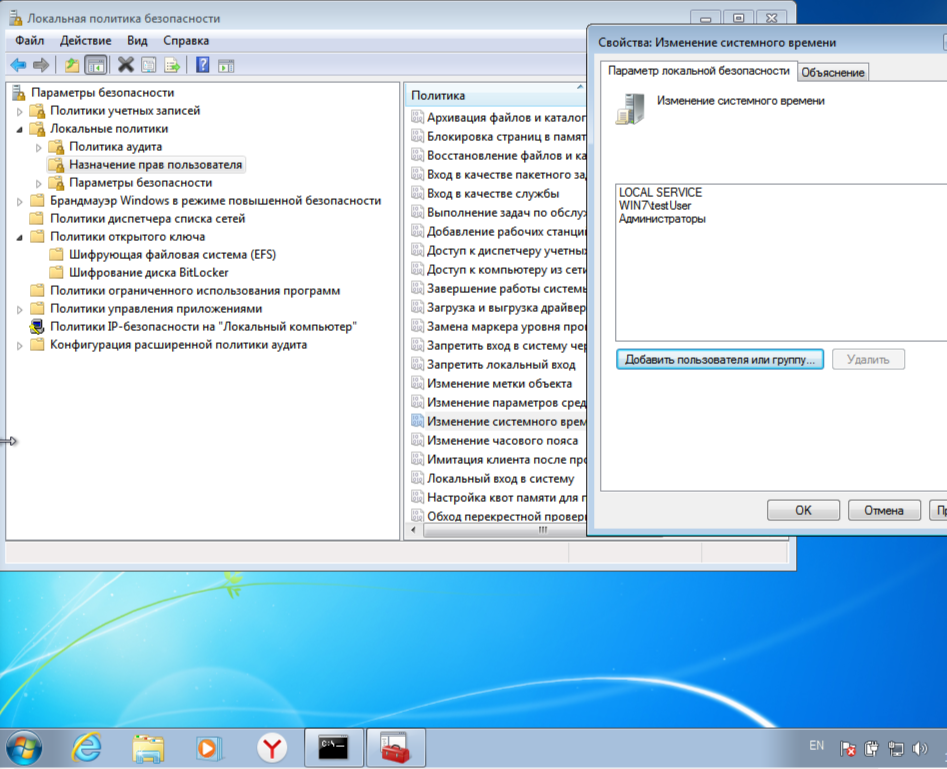


Рисунок 6 – Разрешение политики изменение системного времени

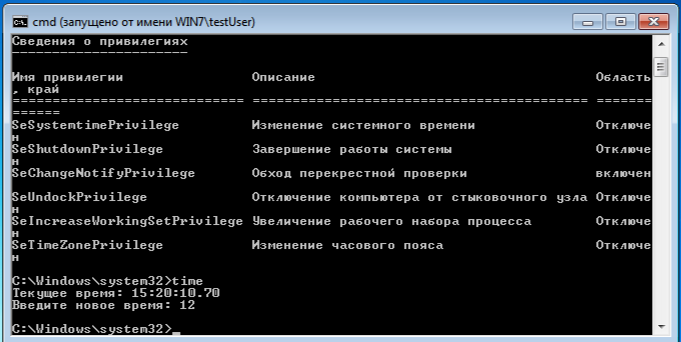


Рисунок 7 - Результат изменения времени

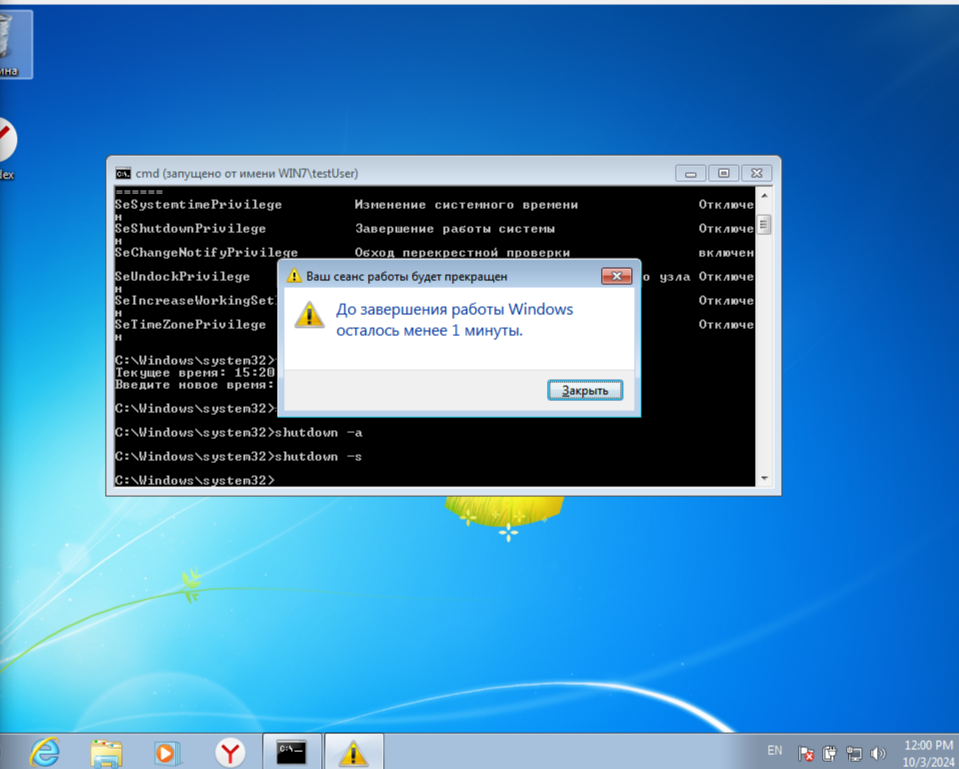


Рисунок 8 – Результат команды shutdown -s

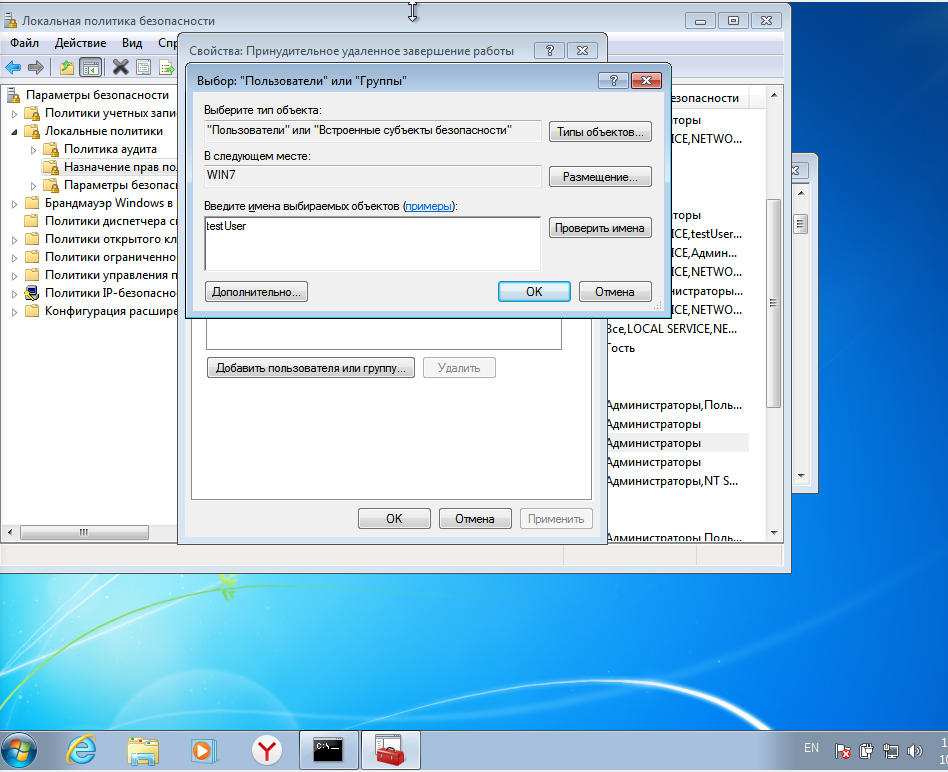


Рисунок 9 – Включение пользователя в политику безопасности



Рисунок 10 – Выдача прав пользователю с помощью команды icacls

icacls "C:\path\to\forTesting" /grant testUser:(W)

icacls "C:\path\to\forTesting" /deny testGroup:(W)



Рисунок 11 – Проверка прав пользователя на чтение

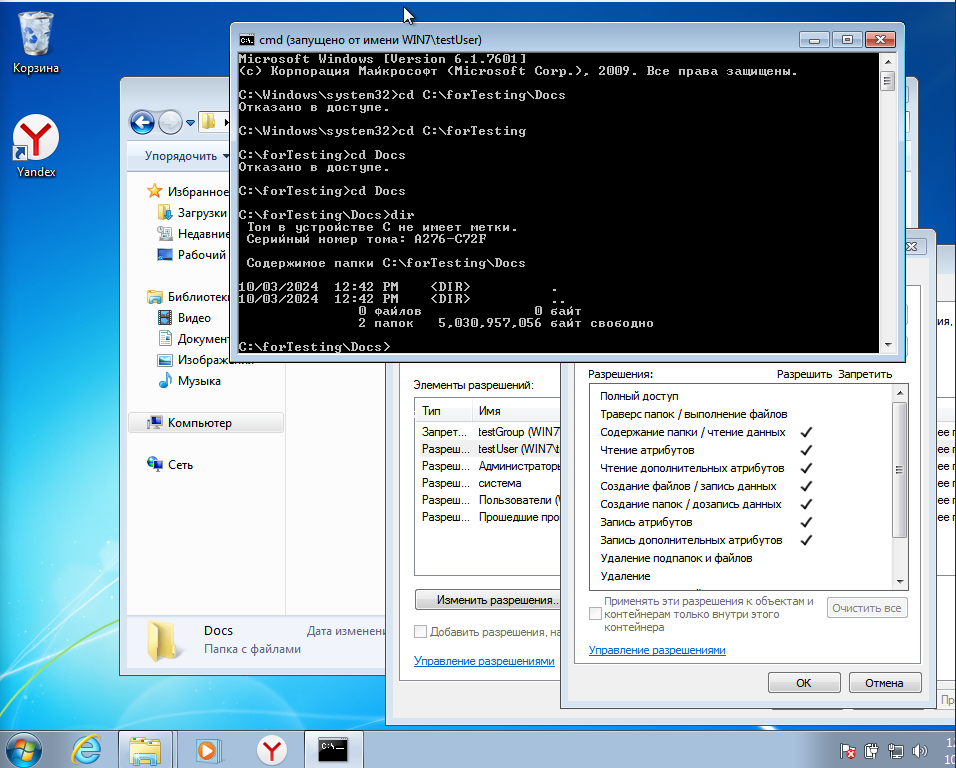


Рисунок 12 – Проверка прав пользователя на чтение

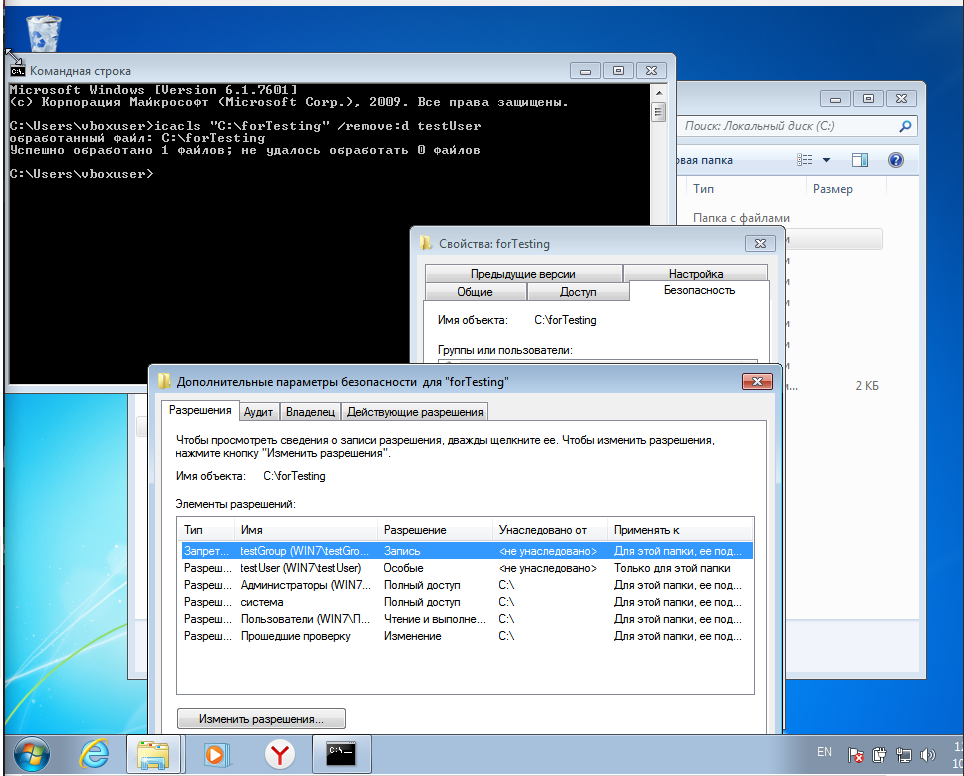


Рисунок 13 – Удаление запрета на чтение

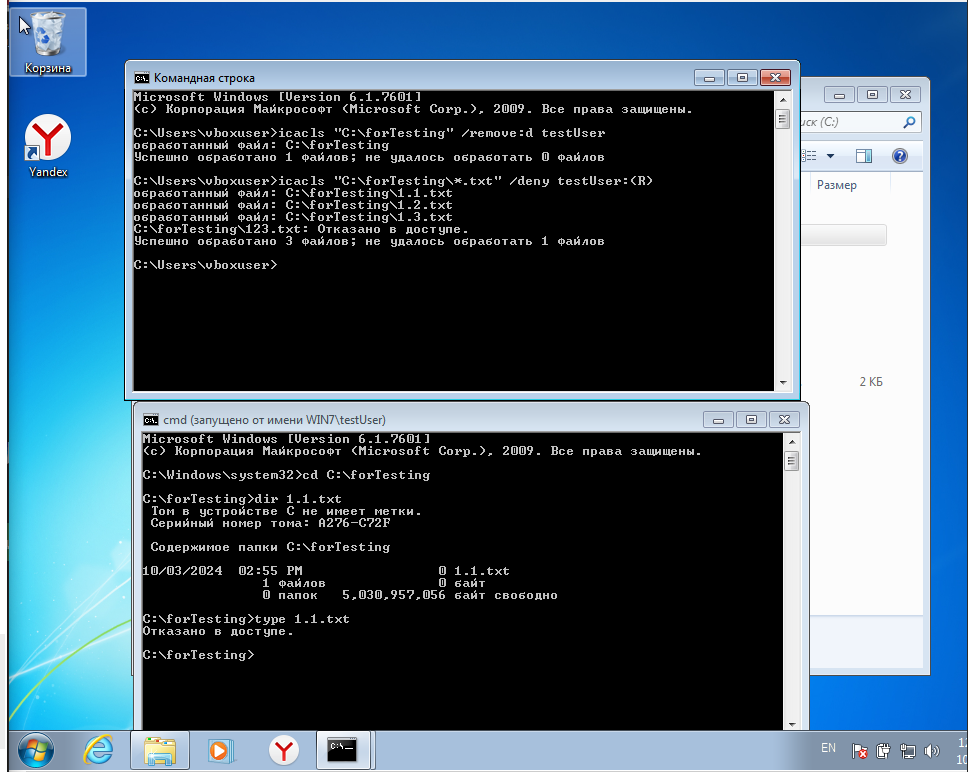


Рисунок 14 – Создание запрета на чтение txt файлов

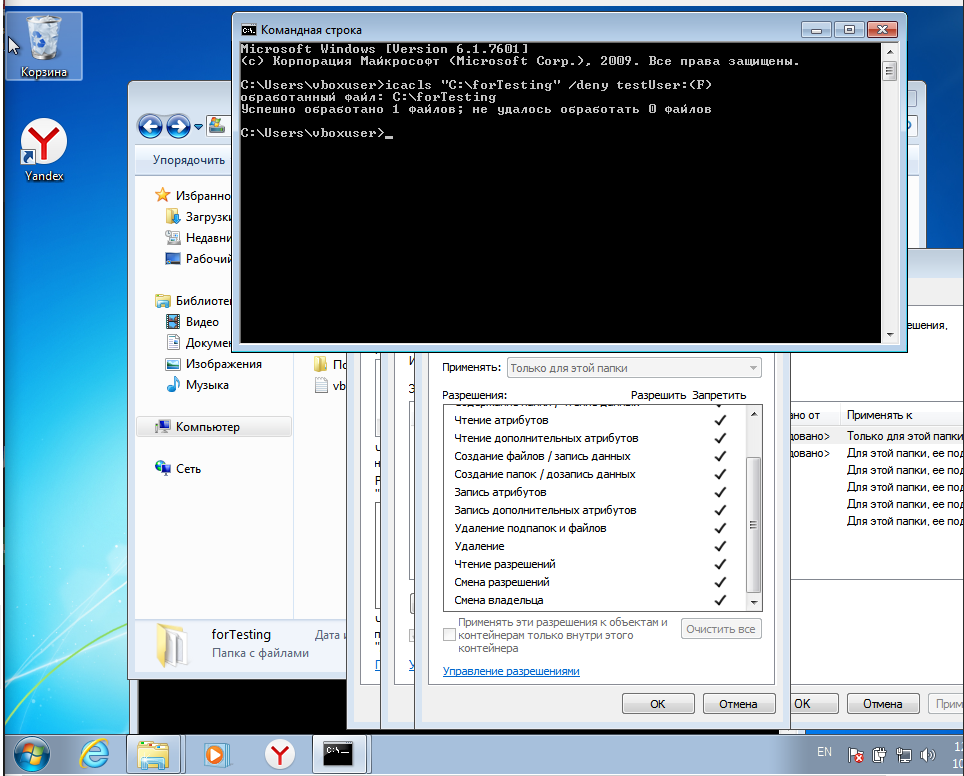


Рисунок 15 – Полный запрет для пользователя

icacls "C:\path\to\forTesting" /deny testUser:(F)

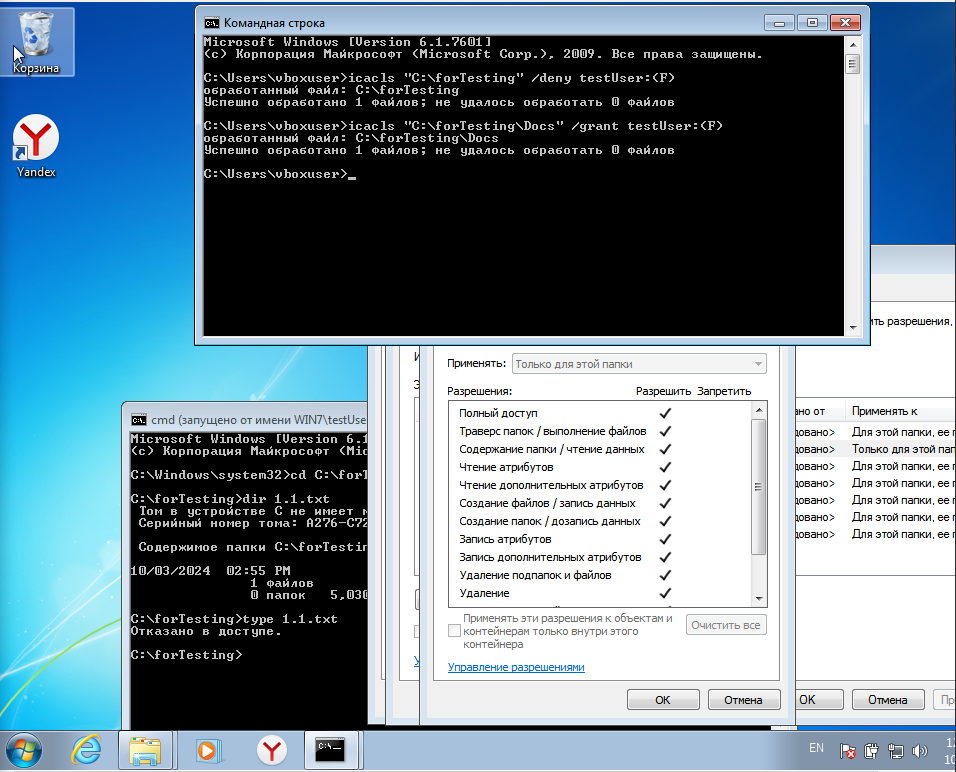


Рисунок 16 – Полный доступ для подпапки

icacls "C:\path\to\forTesting\Docs" /grant testUser:(F)

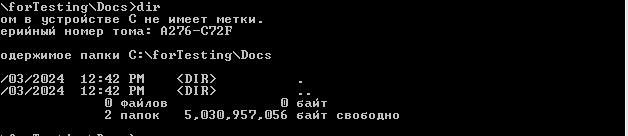


Рисунок 17 – Попытка чтения подпапки

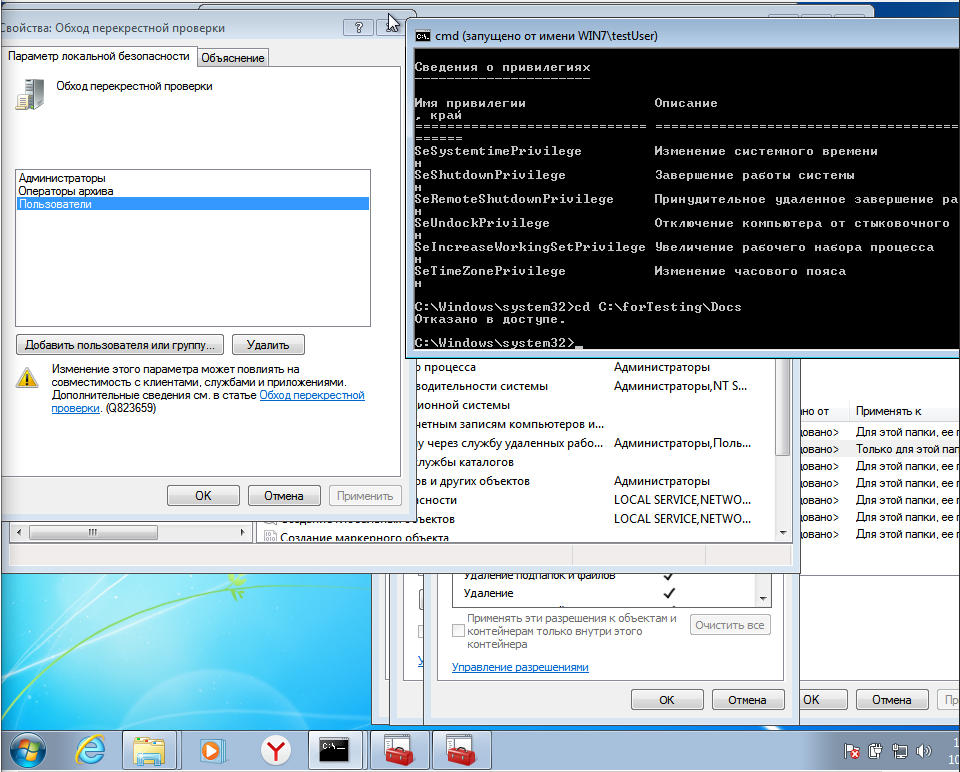


Рисунок 18 – Отключение обхода перекрёстной проверки

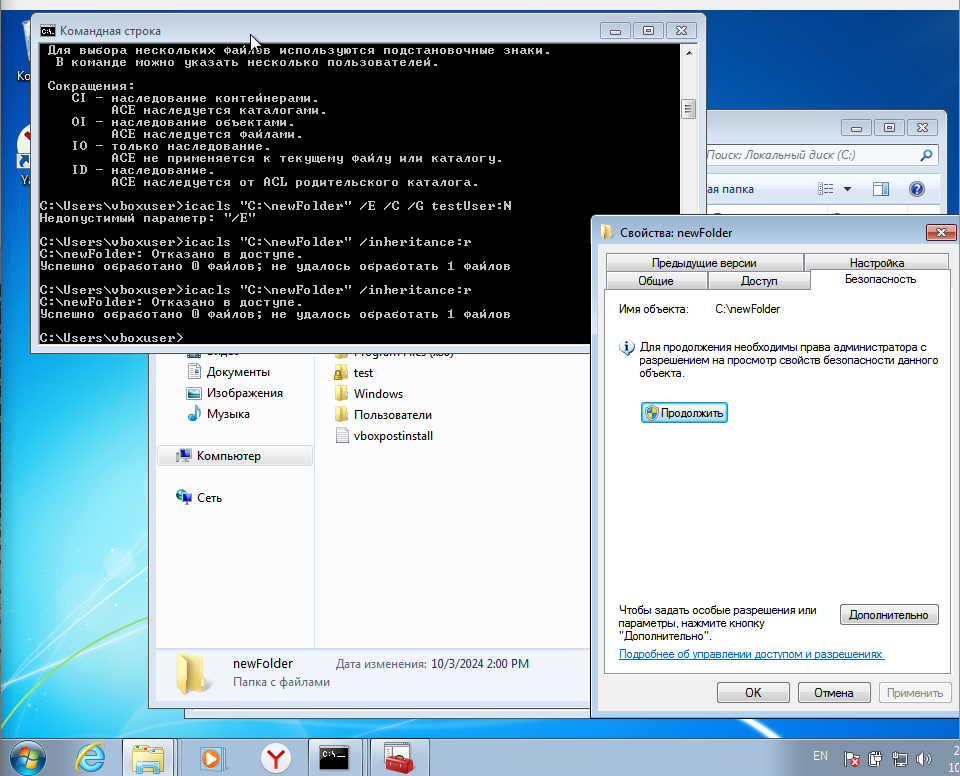


Рисунок 19 – Удаление всех прав на папку

icacls "C:\newFolder" /inheritance:r

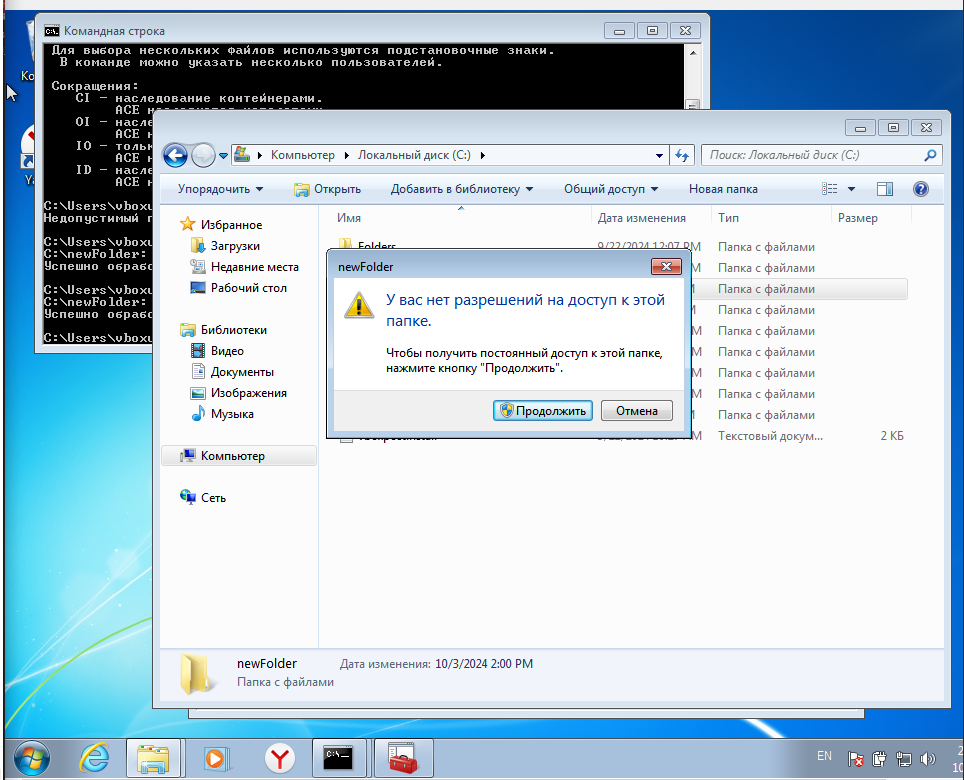


Рисунок 20 – Проверка доступа к папке

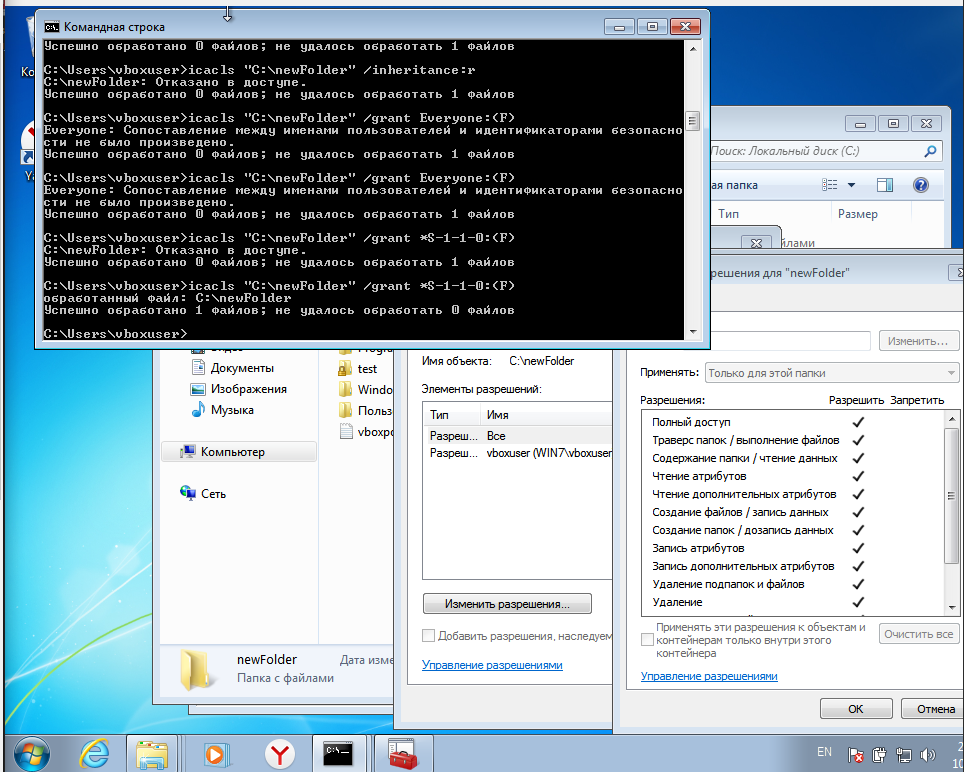


Рисунок 21 – Выдача всем пользователям полного доступа на папку

icacls “C:\newFolder” /grant \*S-1-1-0:(F)

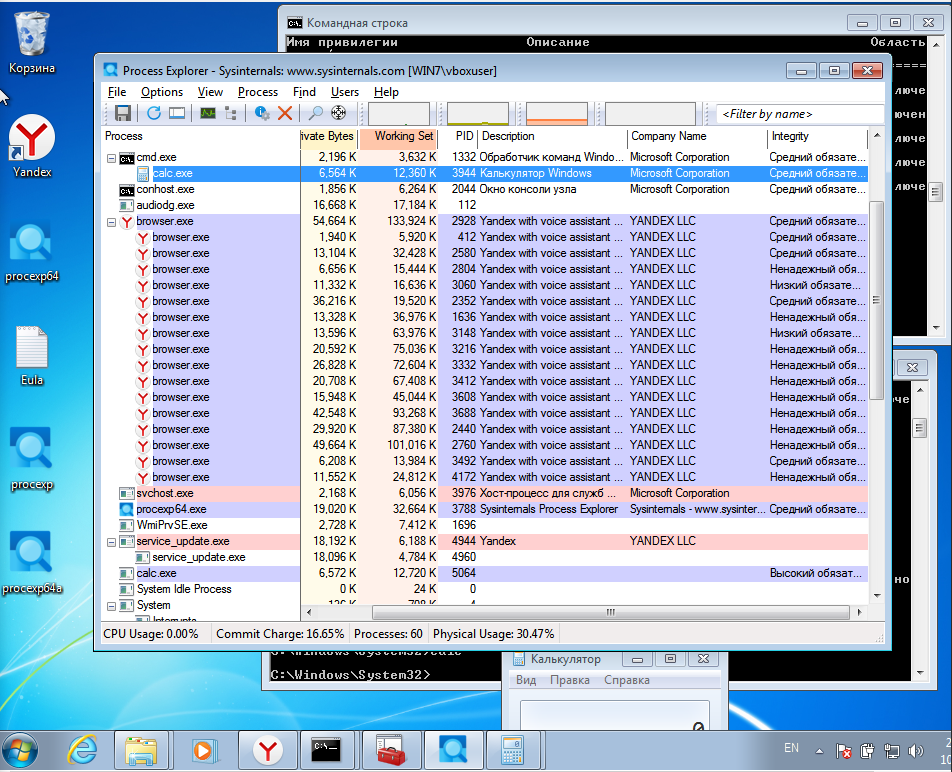


Рисунок 22 – Проверка уровня целостности разных процессов

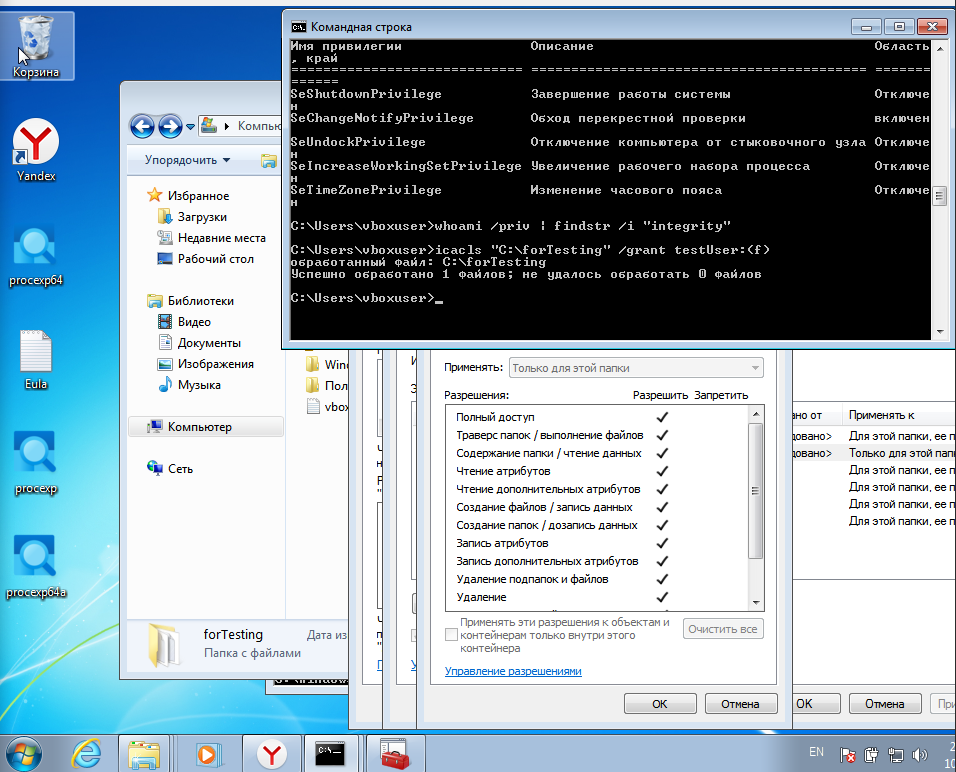


Рисунок 23 – Выдача полного доступа на папку для пользователя

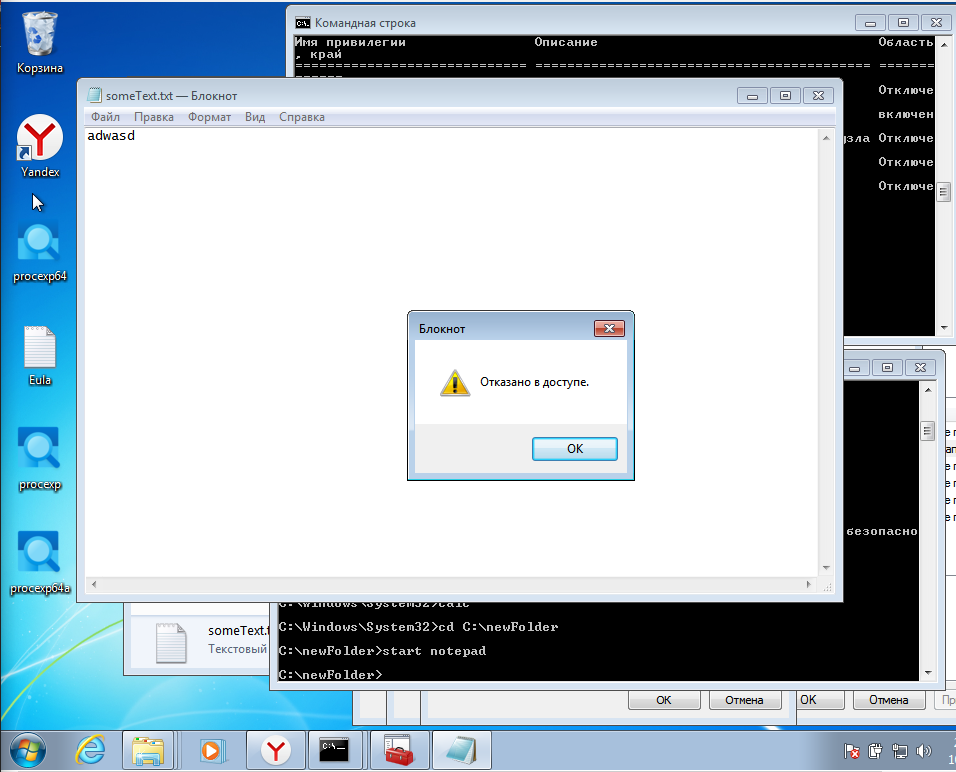


Рисунок 24 – Проверка доступа на запись в папку

1)

C2 «Оранжевой книги». Согласно им, система должна

обеспечивать:

- средство безопасного входа в систему, которое обеспечивают точную

идентификацию пользователей и предоставляют им возможности доступа к

ресурсам компьютера только после прохождения процедуры аутентификации. В

Windows за идентификацию и аутентификацию пользователей отвечают процессы

Winlogon.exe и Lsass.exe.

- управление доступом, позволяющее владельцу ресурса (файла,

раздела реестра, объекта ядра и др.) определить, кто имеет права на доступ к

ресурсу, а также уточнить суть этих прав (чтение, изменение, запуск и т.п.). При

использовании дискреционной модели доступа для уплотнения матрицы доступа

владелец может наделять правами, разрешающими различные виды доступа к

объекту, как отдельного пользователя, так группу пользователей. Безопасный

доступ реализуется в Windows компонентом Security Reference Monitor (SRM,

монитор контроля безопасности) исполнительной системы Ntoskrnl.exe.

- аудит безопасности, позволяющий регистрировать события,

относящиеся к вопросам безопасности. Идентификация пользователей при входе

в систему позволяет привязывать все события безопасности в системе к

конкретному пользователю. В Windows аудит поддерживается SRM и Lsass.exe.

- защита от повторного использования объекта, которая не позволяет

пользователям просматривать данные, удаленные другим пользователем, или не

позволяет обращаться к памяти, которая ранее была использована, а затем

освобождена другим пользователем. В Windows освобожденная память очищается

системным потоком обнуления страниц, работающим во время простоя системы

(с нулевым приоритетом).

2)

**1. Имя пользователя и пароль**

* **Локальные учетные записи**: Пользователи идентифицируются по имени пользователя (логину) и паролю, которые сохраняются на локальном компьютере.
* **Доменные учетные записи**: В доменной среде (например, Active Directory) пользователи идентифицируются по имени пользователя и паролю, которые хранятся на контроллере домена.

**2. Биометрические данные**

* **Отпечаток пальца**: Windows 10 и Windows 11 поддерживают аутентификацию по отпечатку пальца с использованием биометрических считывателей.
* **Распознавание лица**: ОС Windows также поддерживает аутентификацию по распознаванию лица с использованием камеры.

**3. Smart Cards**

* **Смарт-карты**: Пользователи могут использовать смарт-карты для аутентификации. Этот метод часто используется в корпоративных средах для повышения безопасности.

**4. Windows Hello**

* **Windows Hello**: Это технология, которая позволяет пользователям аутентифицироваться с использованием биометрических данных (отпечаток пальца, распознавание лица) или PIN-кода. Windows Hello обеспечивает более безопасную аутентификацию по сравнению с традиционными паролями.

**5. Двухфакторная аутентификация (2FA)**

* **2FA**: Пользователи могут настроить двухфакторную аутентификацию, которая требует ввода пароля и дополнительного фактора, такого как код, отправленный на мобильное устройство.

**6. Аутентификация через Интернет**

* **Microsoft Account**: Пользователи могут использовать учетную запись Microsoft для входа в Windows. Это позволяет синхронизировать настройки и данные между устройствами.
* **OAuth**: В некоторых случаях пользователи могут аутентифицироваться через сторонние сервисы, используя протокол OAuth.

3)

### ****Список управления доступом (DACL)****

**DACL (Discretionary Access Control List)** — это список, который определяет, какие пользователи и группы имеют разрешения на доступ к объекту и какие именно разрешения они имеют. DACL состоит из набора записей управления доступом (ACE), каждая из которых определяет права доступа для конкретного пользователя или группы.

#### Основные характеристики DACL:

* **Разрешения**: DACL определяет, какие действия (например, чтение, запись, выполнение) разрешены или запрещены для конкретных пользователей или групп.
* **Управление доступом**: Владелец объекта может изменять DACL, чтобы предоставить или ограничить доступ к объекту.
* **Наследование**: DACL может наследоваться дочерними объектами, что позволяет автоматически применять разрешения к новым объектам, созданным в контейнере (например, папке).

#### Пример:

Если DACL для файла указывает, что пользователь "Alice" имеет разрешение на чтение и запись, а пользователь "Bob" имеет только разрешение на чтение, то "Alice" сможет изменять файл, а "Bob" — только читать его.

### 2. ****Список аудита доступа (SACL)****

**SACL (System Access Control List)** — это список, который определяет, какие события доступа к объекту должны быть зарегистрированы в журнале событий безопасности. SACL также состоит из набора записей управления доступом (ACE), каждая из которых определяет, какие действия и для каких пользователей или групп должны быть зарегистрированы.

#### Основные характеристики SACL:

* **Аудит**: SACL позволяет администраторам отслеживать попытки доступа к объекту, независимо от того, были ли они успешными или нет.
* **Типы событий**: SACL может регистрировать различные типы событий, такие как успешные попытки доступа, неудачные попытки доступа, или оба типа.
* **Наследование**: SACL может наследоваться дочерними объектами, аналогично DACL.

5)

### 1. ****Идентификация и аутентификация пользователя****

* **Идентификация**: Определение того, кто пытается получить доступ к ресурсу. Это может быть локальный пользователь или пользователь из доменной среды.
* **Аутентификация**: Проверка подлинности пользователя с использованием имени пользователя и пароля, биометрических данных, смарт-карт или других методов.

### 2. ****Получение маркера доступа (Access Token)****

* После успешной аутентификации система создает **маркер доступа** (Access Token), который содержит информацию о пользователе, включая его идентификатор безопасности (SID), членство в группах и привилегии.
* Этот маркер доступа используется для проверки прав доступа к ресурсам в течение всего сеанса работы пользователя.

### 3. ****Проверка прав доступа с использованием DACL****

* **DACL (Discretionary Access Control List)**: Каждый защищаемый объект (например, файл, папка, реестр) имеет DACL, который определяет, какие пользователи и группы имеют разрешения на доступ к объекту.
* **ACE (Access Control Entry)**: DACL состоит из набора записей ACE, каждая из которых определяет права доступа для конкретного пользователя или группы.

6)

Маркер безопасности — это объект, который содержит информацию о пользователе или процессе, включая их идентификаторы безопасности (SID), членство в группах, привилегии и другие атрибуты безопасности. Этот объект создается операционной системой после успешной аутентификации пользователя и используется для проверки прав доступа к ресурсам и выполнения операций в системе.

### Содержимое маркера безопасности

Маркер безопасности обычно содержит следующую информацию:

1. **Идентификатор безопасности пользователя (SID)**: Уникальный идентификатор, который идентифицирует пользователя в системе.
2. **Идентификаторы безопасности групп (Group SIDs)**: Уникальные идентификаторы групп, в которые входит пользователь.
3. **Привилегии (Privileges)**: Список привилегий, которые пользователь имеет в системе (например, право изменять системные часы, завершать работу системы).
4. **Атрибуты безопасности**: Дополнительные атрибуты, такие как информация о сеансе, ограничения на использование привилегий и другие.

8)