Титулка

**Мета роботи:** ознайомитися з основними поняттями в галузі політик в середовищі сучасних операційних систем, основними засобами безпеки у сучасних операційних системах. Набути практичних навичок в роботі по налаштуванні політик безпеки ОС Windows.

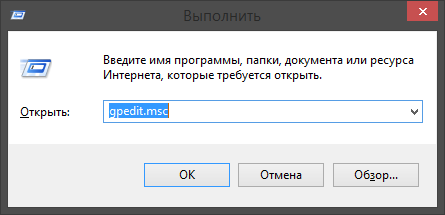
**Завдання роботи**: ознайомитися з засобами безпеки, наявними у складі операційних систем Windows та Linux. Налаштувати політики безпеки ОС Windows відповідно до порядку виконання лабораторної роботи.

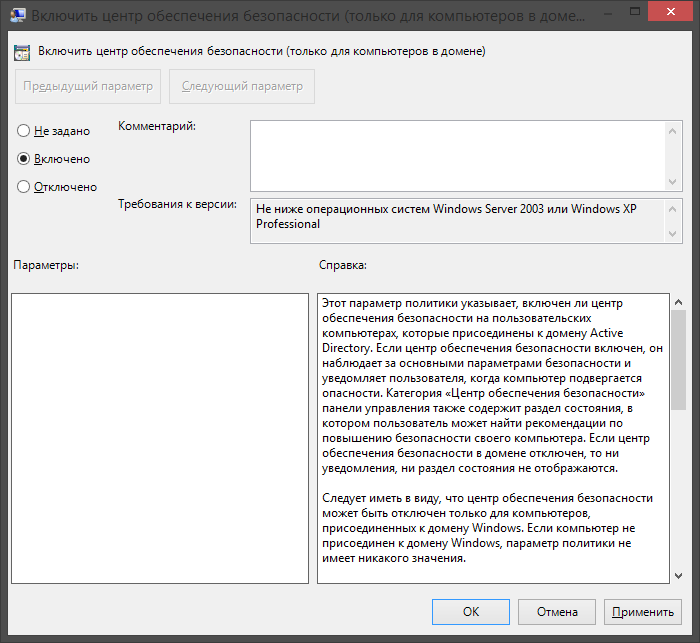
# Хід роботи

## Увімкнення Центру забезпечення безпеки Windows

Щоб увімкнути Центр забезпечення безпеки Windows, необхідно запустити Редактор групової політики. Для цього натискаємо комбінацію клавіш Win + R і вводимо «gpedit.msc».

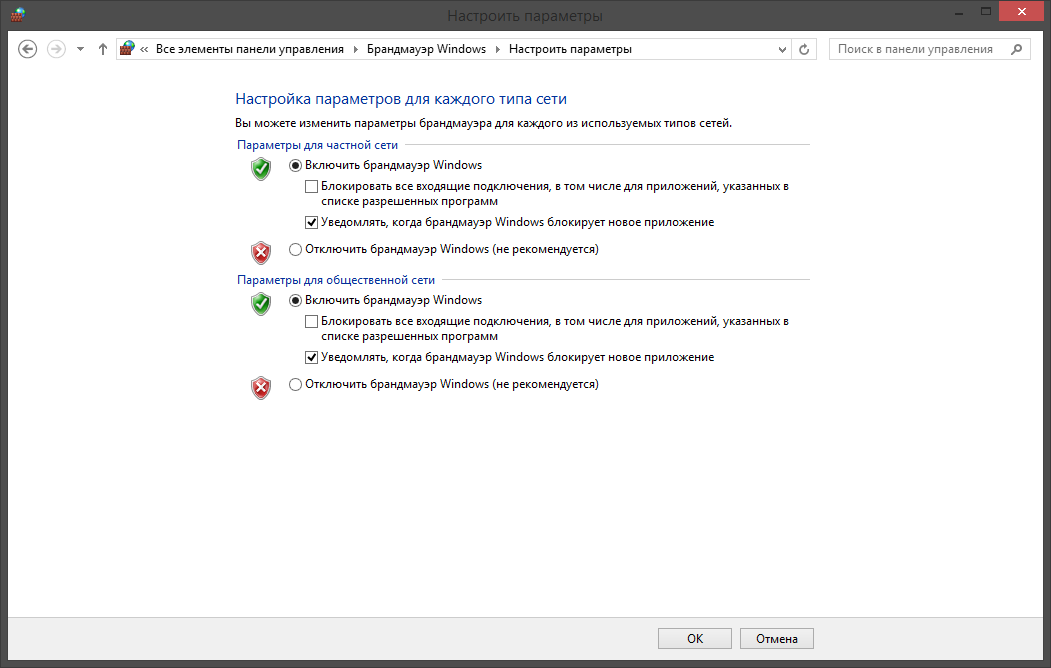
Запустивши Редактор групової політики, переходимо до вузла «Конфігурація комп’ютера» → «Адміністративні шаблони» → «Компоненти Windows» → «Центр забезпечення безпеки» і вмикаємо політику «Увімкнути центр забезпечення безпеки (тільки для комп’ютерів домена)». В результаті був увімкнений Центр забезпечення безпеки.

  
Рисунок 1: Запуск Редактора групової політики

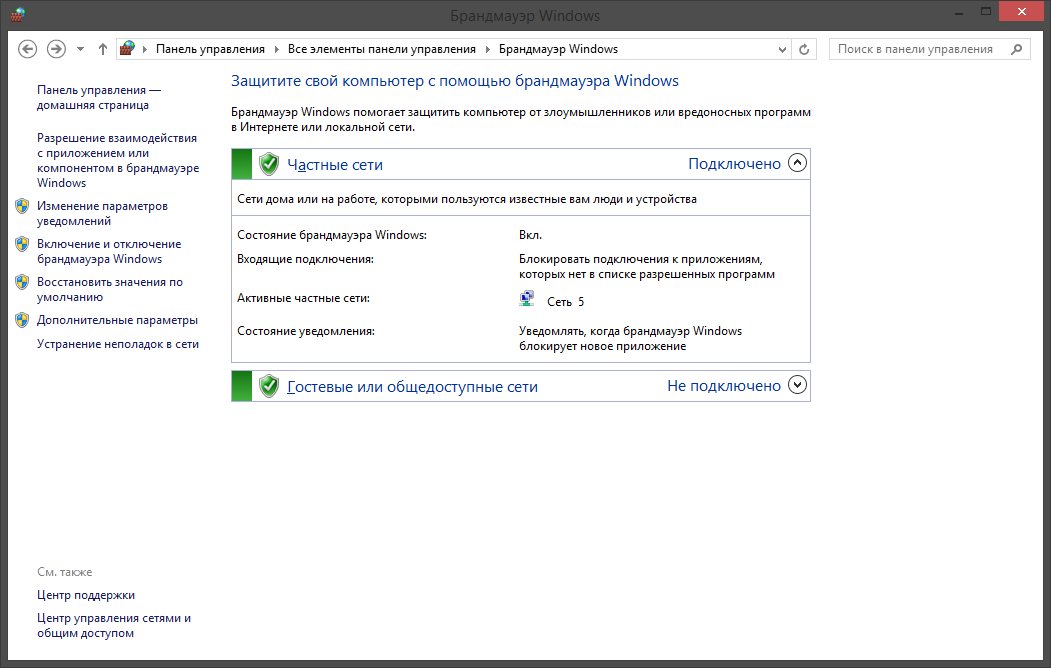
  
Рисунок 2:

## Запуск Брандмауера Windows

Щоб запустити Брандмауер Windows, треба натиснути кнопку «Пуск» → «Панель управління» → «Брандмауер Windows». Відкривши це вікно, можна вимкнути або увімкнути Брандмауер.

  
Рисунок 3: вікно, яке дозволяє увімкнути або вимкнути брандмауер

Після увімкнення брандмауера, його можна використовувати.

  
Рисунок 4: вікно увімкненого брандмауера

## Запуск захисника Windows. Розгляд параметрів попередження про погрози. Захист в реальному часі

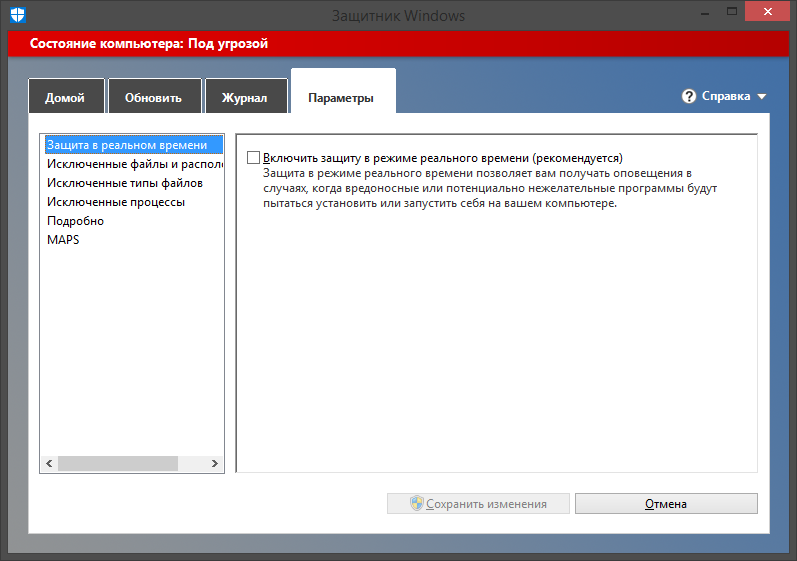
Щоб запустити Захисника Windows, відкриваємо Панель керування та обираємо пункт «Захисник Windows». Переходимо у вкладку «Параметри», де доступні такі параметри:

1. Захист в реальному часі.
2. Виняткові файли і розміщення.
3. Виняткові типи файлів.
4. Виняткові процеси.
5. Детально.
6. MAPS.

Параметри «виняткові файли і розміщення», «виняткові типи файлів» і «виняткові процеси» відповідають за попередження про загрози: вони налаштовують, які об’єкти Захисник Windows має ігнорувати, а тому і не попереджати користувача.

Бачимо параметр «Увімкнути захист у режимі реального часу».

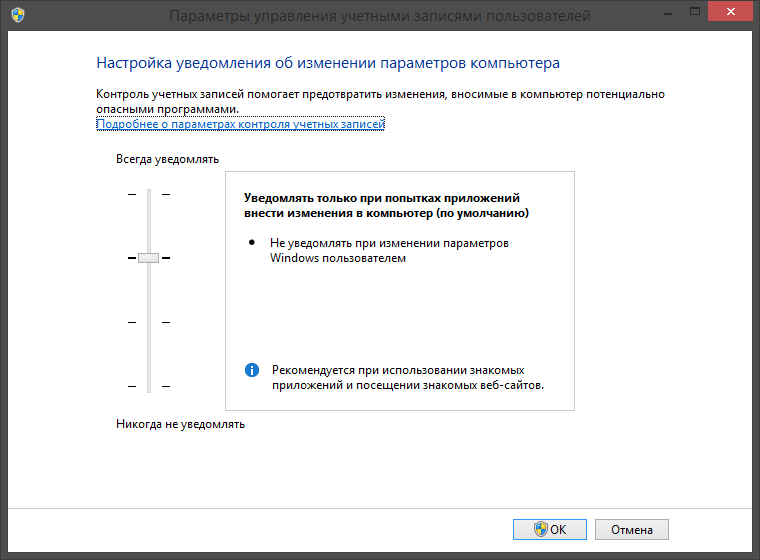
Якщо цей параметр увімкнений, Захисник Windows буде попереджати користувача щоразу, коли зловмисна програма намагатиметься встановити себе на локальний комп’ютер. Щоб увімкнути цей параметр, необхідно встановити прапорець навпроти його.

  
Рисунок 5: параметри Захисника Windows

## Налаштування UAC

Щоб налаштувати UAC (User Access Control, контроль облікових записів), необхідно відкрити Панель керування, перейти у Центр підтримки і натиснути на кнопку «Зміна параметрів контролю облікових записів» у боковому меню. Тоді відкриється вікно контролю облікових записів.

Як видно у цьому вікні, контроль облікових засобів дозволяє повідомляти користувача про зміни параметрів комп’ютера відповідно до 4 рівнів безпеки:

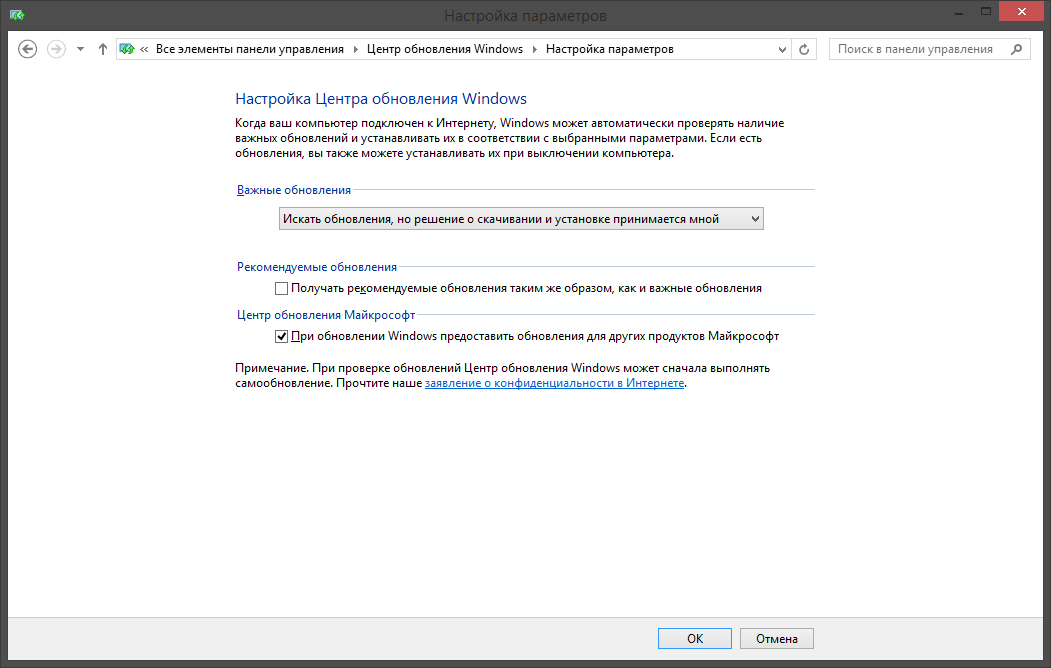
  
Рисунок 6: вікно налаштувань контролю облікових засобів

1. Не повідомляти — ніколи не повідомляти про зміни.
2. Повідомляти при спробах додатків внести зміни в комп’ютер (не затемнювати робочий стіл) — не повідомляти, коли поточний користувач вносить зміни.
3. Повідомляти при спробах додатків внести зміни в комп’ютер — не повідомляти, коли користувач вносить зміни.
4. Завжди повідомляти — повідомляти щоразу, коли додатки намагаються встановити програмне забезпечення або змінити параметри комп’ютера або коли користувач змінює параметри комп’ютера.

## Налаштування Центру оновлення Windows

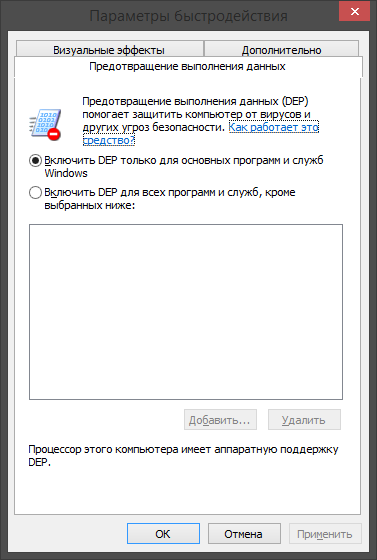
В операційній системі Windows 8.1 налаштування Центру оновлення Windows знаходиться за шляхом Панель керування → Центр оновлення Windows. У лівій частині цього вікна з’явиться кнопка «Налаштування параметрів». Натиснувши на неї, з’явиться вікно налаштування параметрів Центру оновлення Windows.

Керування функцією DEP

  
Рисунок 7: параметри Центру оновлення Windows

Вікно для керування функцією DEP знаходиться за шляхом Панель керування → Система → Властивості системи → Додаткові параметри → Параметри швидкодії, вкладка «Запобігання виконанню даних». Функція DEP (Data Execution Prevention) допомагає заблокувати виконання шкідливого коду, навіть якщо зловмисник зміг використати певну вразливість і впровадити його у довірену програму.

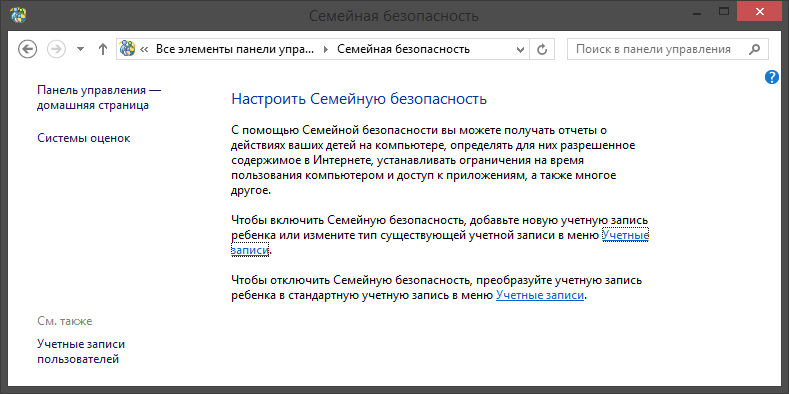
У цьому вікні можна налаштувати, в яких випадках буде працювати функція DEP: лише для основних програм і служб Windows чи для всіх програм, окрім явних винятків.

  
Рисунок 8:

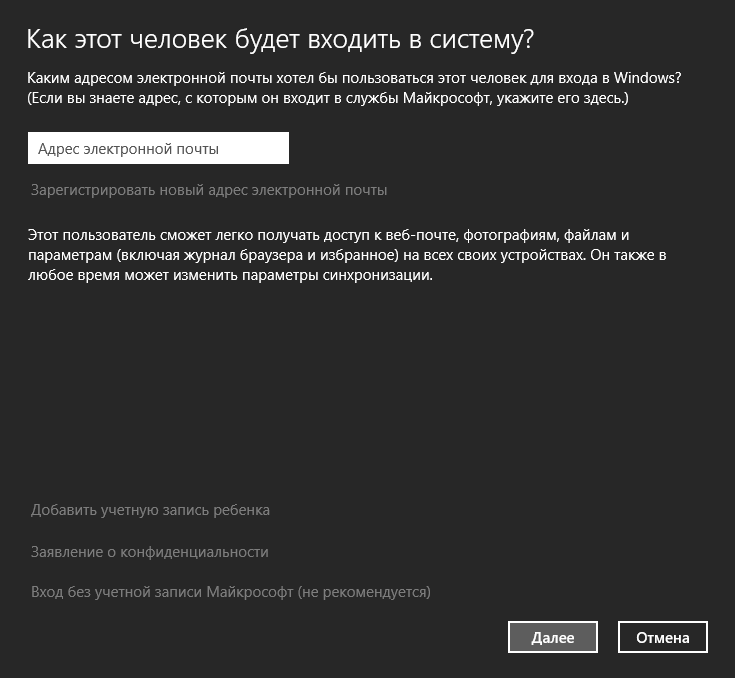
## Батьківский контроль

Примітивний опис інструментів батьківського контролю знаходяться за шляхом Панель керування → Сімейна безпека.

Однак, основний інструментарій вбудований в облікові записи Windows. Щоб використати інструменти батьківського контролю, досить перейти в меню «Обліковий записи», і створити обліковий запис дитини обмежений правилами батьківського контролю.

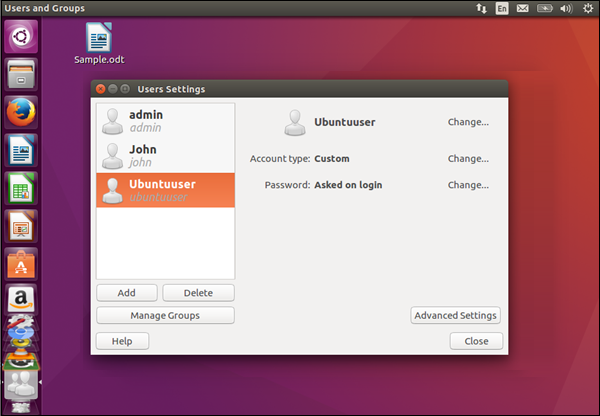
  
Рисунок 9:

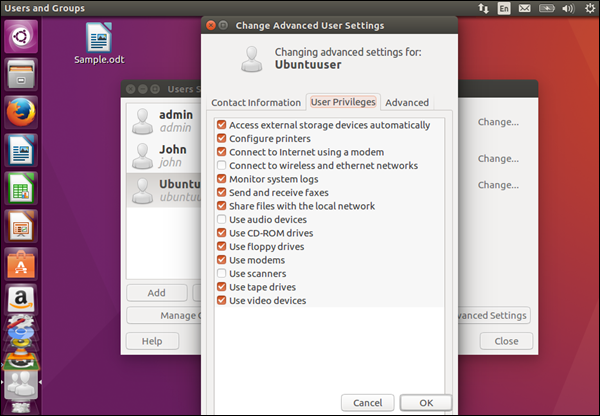
## Керування користувачами та групами в Linux

  
Рисунок 10: вікно створення облікового запису Windows. Внизу є можливість створити обліковий запис дитини, обмежений засобами батьківського контролю

Запускаємо панель «Керування користувачами та групами». Ця панель надає можливості створювати користувачів і групи, а також налаштовувати їх параметри.

За допомогою цієї панелі можна також виконати детальне налаштування кожного користувача, натиснувши кнопку «Розширені налаштування», де можна увімкнути доступ до зовнішніх носіїв інформації, налаштування принтерів.

  
Рисунок 11: панель «Користувачі та групи»

  
Рисунок 12: детальні налаштування користувача в меню «Користувачі та групи»

## Перевірка можливостей роботи з обліковими записами

У встановленій версії Linux є можливість вимагати від користувача зміни пароля через певний термін за допомогою командного рядка. Для цього необхідно виконати команду chage з бажаними параметтрами. Щоб налаштувати спосіб шифрування паролю, можна виконати у командному рядку команду chpasswd --crypt-method METHOD. У вибраній версії Ubuntu LiveCD можна налаштувати менеджер входу в систему за допомогою команд chsh (змінити оболонку), chfn (змінити деталі).

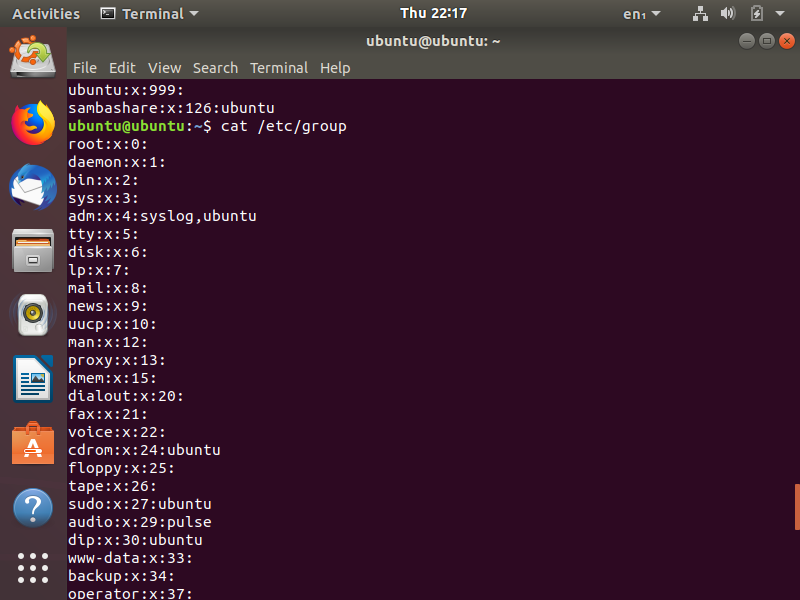
Системні групи та фіктивні користувачі

Взагалі, немає чіткого розподілу груп в Linux на «системні» і «не системні», однак, зазвичай користувацькі групи позначають з ID більшим за 1000. Щоб вивести перелік усіх груп, необхідно виконати таку команду:

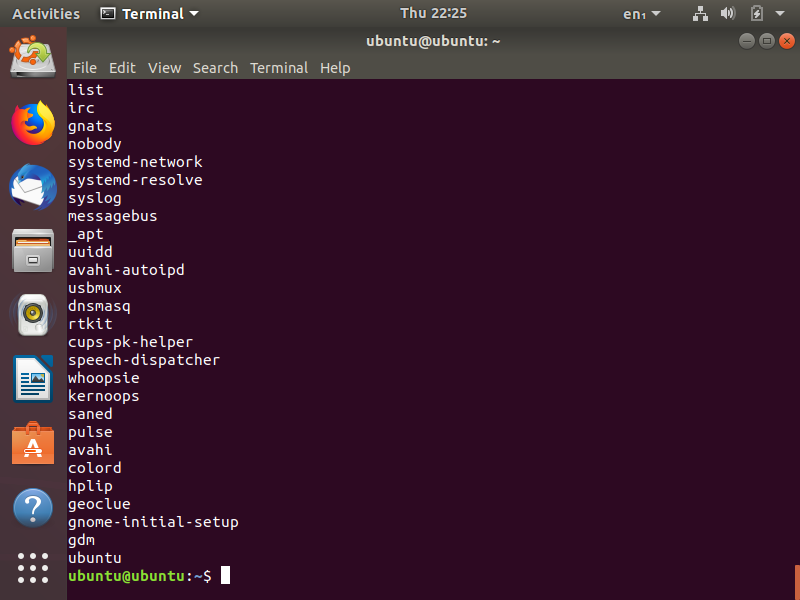
cat /etc/group

В результаті отримаємо перелік груп.

Тепер виведемо список користувачів, виконавши таку команду:

  
Рисунок 13: перелік груп в операційній системі

cat /etc/passwd

  
Рисунок 14: список користувачів операційної системи

Тепер розглянемо групи і одноіменних користувачів, які зазвичай вважають системними:

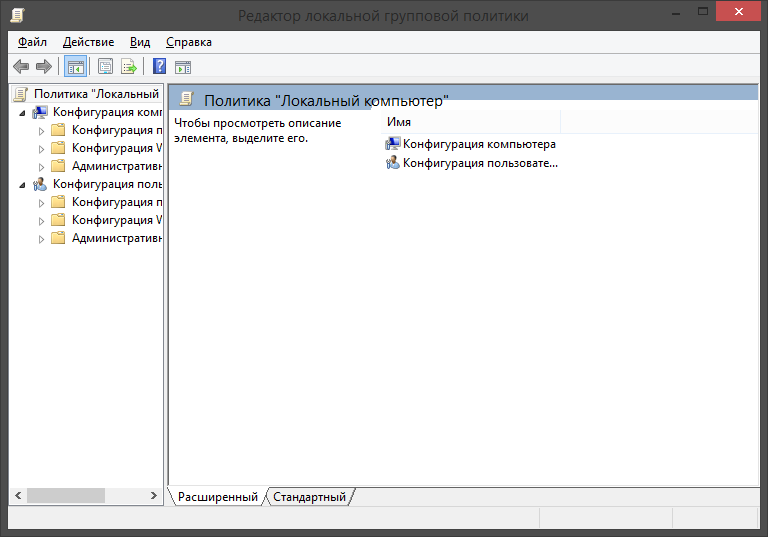
|  |  |
| --- | --- |
| Root | Суперкористувач |
| Daemon | Фонові програми |
| Bin | Застаріла група для виконуваних програм |
| Adm | Надаються привілеї для адміністрування |
| Lp | Надаються привілеї для принтерів |
| Sync | Вхід для синхронізації системи |
| Shutdown | Вимкнення системи |
| Halt | Зупинка системи |
| Mail | Пошта |
| News | Новини |
| Uucp | Спеціальні привілеї для UUCP (копіювання між системами Unix) |
| Operator | Спеціальні привілеї для операторів системи (застаріле) |
| Man | Спеціальні привілеї для інструкцій до програм |
| Nobody | Користувач-ніхто, використовується файловою системою NFS |

Взагалі, у груп і користувачів відсутні права в загальному сенсі, їм лише надають доступ до певних файлів і директорій окремо, тому переглянути права групи чи користувача неможливо.

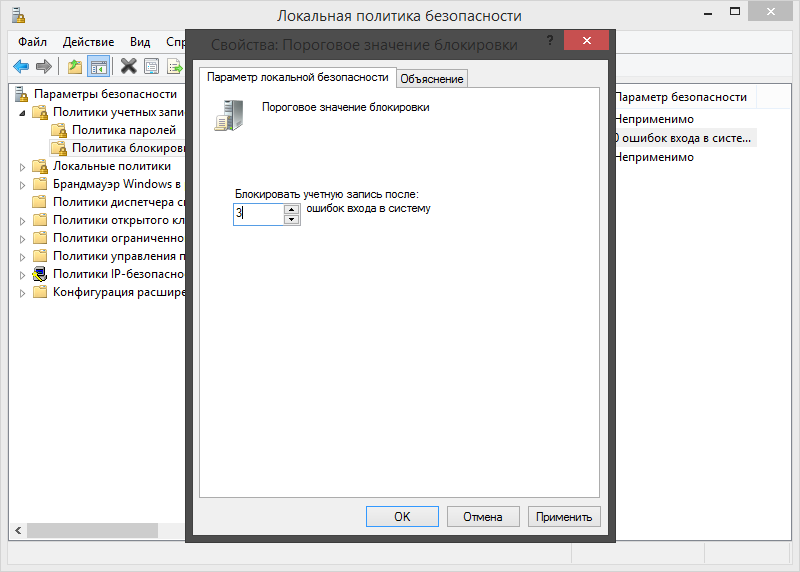
## Знайомство з Редактором локальної групової політики

Редактор локальної групової політики дозволяє керувати опціями політик безпеки.

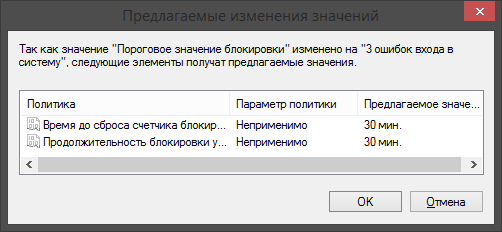
Підрозділом цього редактора є Локальна політика безпеки, доступна за шляхом Панель керування → Адміністрування → Локальна політика безпеки. За допомогою Локальної політики безпеки можна змінювати параметри, які застосуються для управління паролями облікових записів. Наприклад, обмежимо кількість некоректних спроб входу 3 спробами.

  
Рисунок 15: вікно Редактора локальної політики безпеки

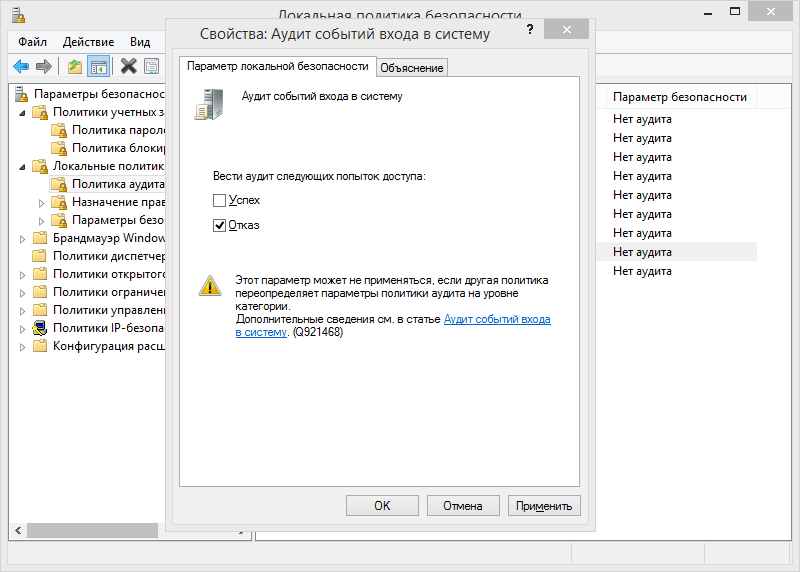
Також вкажемо час тривалості блокування, а також тривалість, після якого обліковий запис розблокується

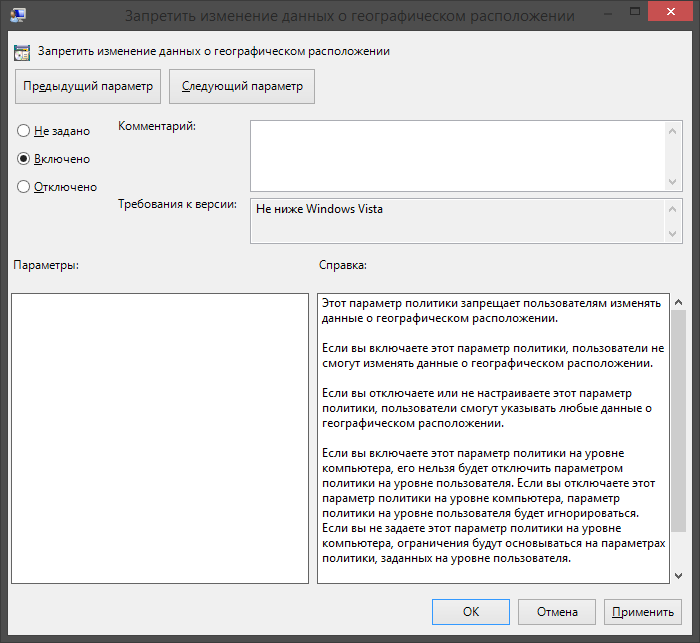
  
Рисунок 16: обмеження кількості некоректних спроб входу

Налаштовуємо політику для того, щоб під час кожної невдалої спроби входу створювався запис аудиту.

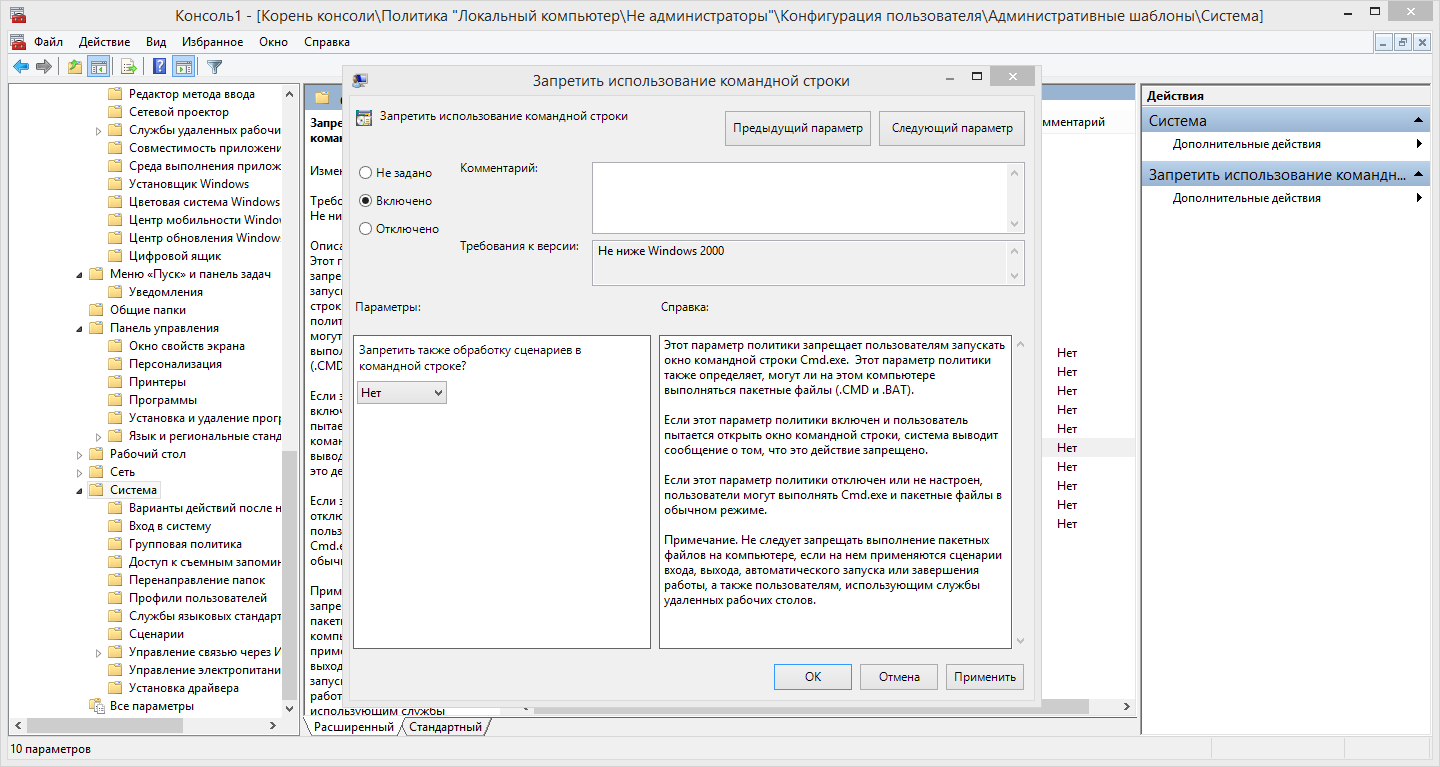
  
Рисунок 17: встановлення параметрів розблокування

Тепер заборонимо користувачам змінювати дані про своє географічне положення. Для цього переходимо в Конфігурацію комп’ютера → Адміністративні шаблони → Система → Служби мовних стандартів → Заборонити зміну даних про географічне розташування.

  
Рисунок 18: налаштування для створення запису аудиту щоразу, коли користувач виконує невдалу спробу увійти в систему

  
Рисунок 19: вікно налаштування заборони зміни даних про географічне розташування

Тепер заборонимо використовувати командний рядок.

  
Рисунок 20: вікно, де можна заборонити користуватись командним рядком