Лобанчикова Н

Практичне заняття № 7

НАЛАШТУВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ОПЕРАЦІЙНОЇ СИСТЕМИ Windows 10 ІЗ ЗАСТОСУВАННЯМ ПРОГРАМИ VirtualBox

Мета: отримання практичних навичок з налаштування параметрів безпеки операційної системи Windows 10 із застосуванням програми VirtualBox

ТЕОРЕТИЧНІ ВІДОМОСТІ

Для виконання даної лабораторної роботи необхідно встановити програму для віртуальних машин Oracle VM VirtualBox (http://surl.li/amwgc) та імпортувати в неї образ Windows 10 (https://drive.google.com/file/d/1mcqokjer5sHGIObJXaoY-FHhUcfZO4UC/view?usp=sharing).

Провести перейменування Віртуальної машини за зразком: W10_Прізвище_група. Використовуємо при вході в ОС **логін: Student, пароль 1111**. Результат проведеної роботи представлено на рис.1.

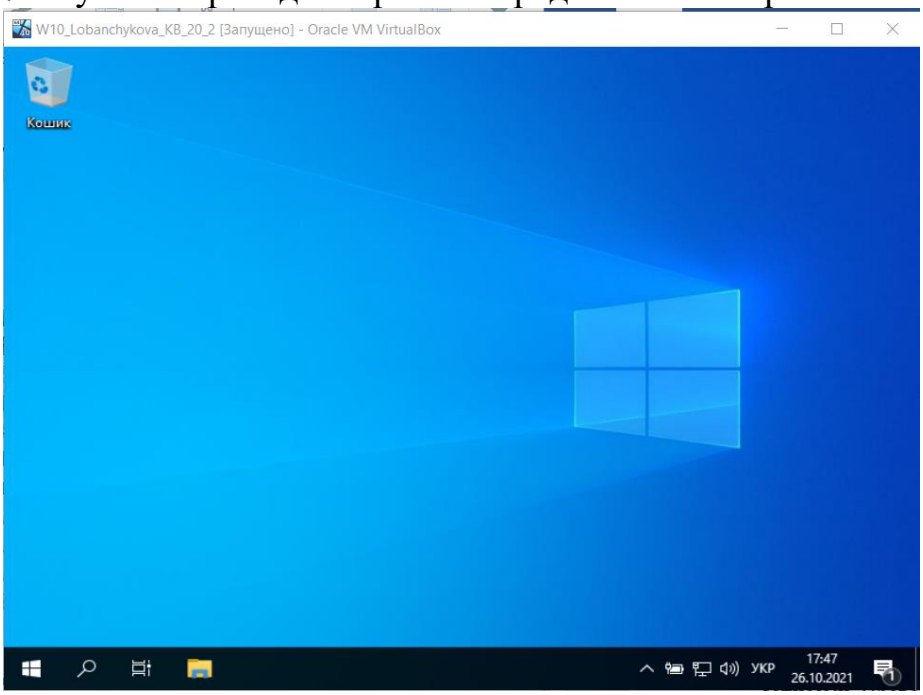

Рис.1

1. Оновлення

Враховуючи те, що при налаштуванні віртуальної машини (ВМ) один із адаптерів включено у режимі використання NAT, ВМ отримала від хостової один із IP-адрес, що дозволяє нам отримати доступ до Інтернету, рис.2, що відповідно робить можливим процес інсталювання.

Після інсталяції операційної системи, переконайтеся, що встановлено всі доступні оновлення. Це захистить та забезпечить виправлення помилок, а також закриє існуючі вразливості ОС. Для цього необхідно вибрати «Інсталювати оновлення та перезавантажити», рис.3.

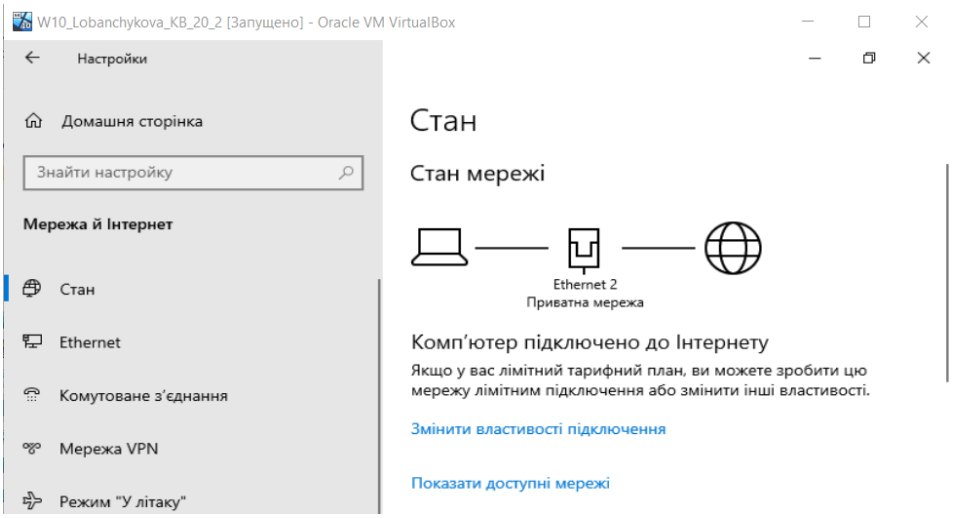

Рис. 2 – Параметри мережі ВМ

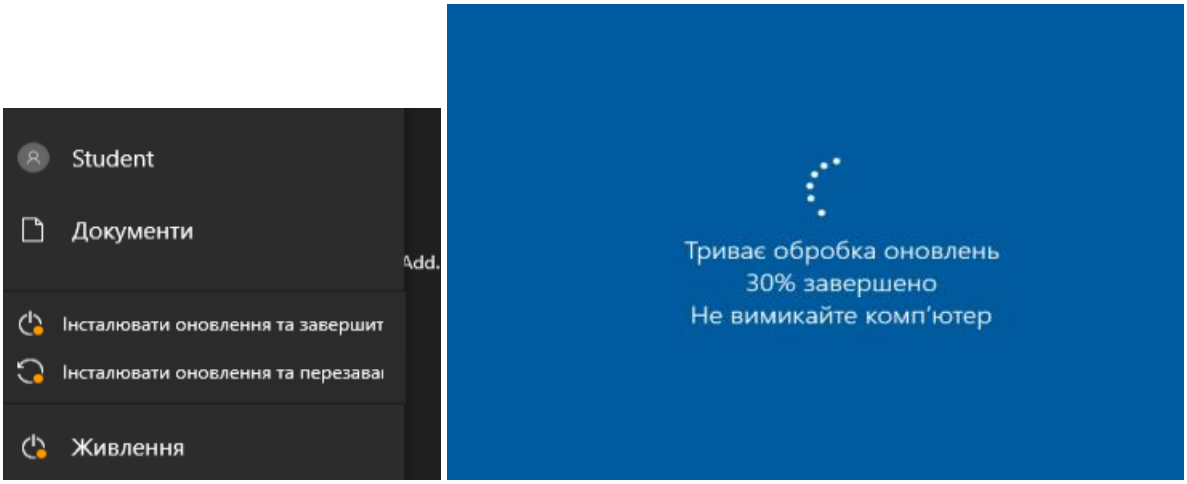

Рис. 3 – Встановлення оновлень

1.2. Антивірусний захист

Наступним кроком є встановлення антивірусного програмного забезпечення. Вибір даного типу програмного продукту досить широко представлено на ринку. Тому необхідно провести аналіз та встановити антивірусну програму. Результати роботи представити у вигляді скріншоту.

1.3. Облікові записи

Одним із засобів безпеки ОС Windows 10 є управління обліковими записами. Проведемо дослідження даної технології. Створимо додатковий обліковий запис для повсякденної роботи для підвищення рівня безпеки ОС та уникнення потенційних проблем при роботі під обліковим записом з підвищеними привілеями.

Для цього необхідно запустити файловий провідник, рис. 4 → Мій комп'ютер → правою кнопкою миші елемент Керування, рисунок 5.

Рис. 4 – Вибір параметру «Керування»

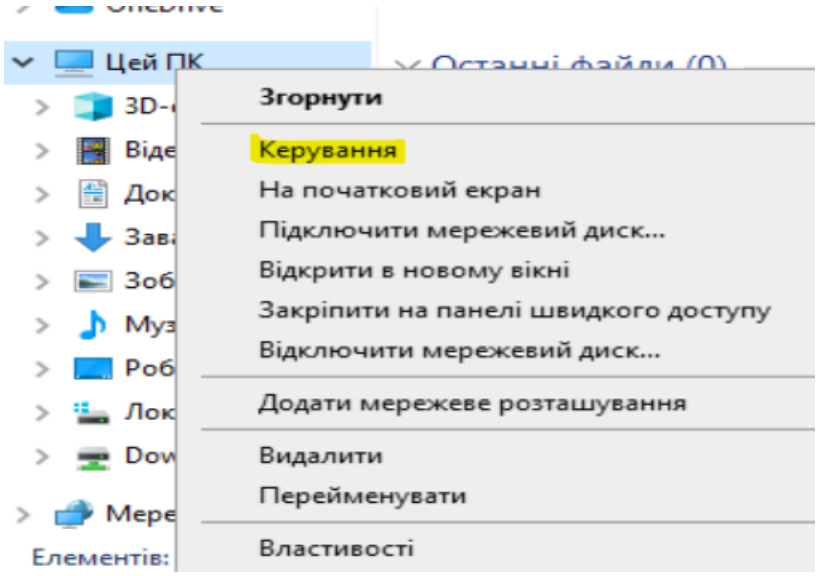

Рис.5 – Вибору елементу «Керування»

У вікні, що відкриється вибрати : «Локальні користувачі»-«Користувачі», рисунок 6.

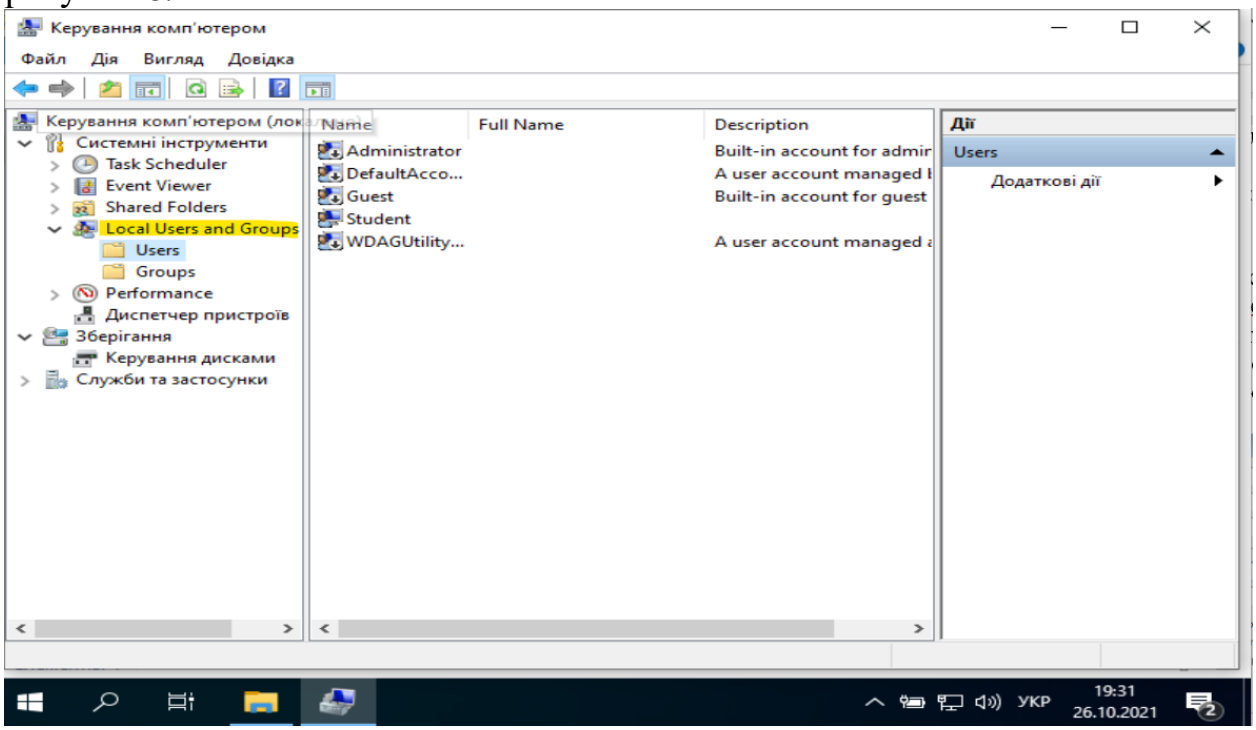

Рис. 6 – Вікно керування користувачами

Далі необхідно перейти у вікно «Дії», натиснути «Додаткові дії»→ «Новий користувач», рис. 7.

Створити користувача, в моєму випадку це **Student 2**. Це буде ваш обліковий запис користувача для повсякденного використання. Заповнюємо поля та натискаємо «Створити», рис.8. По замовчуванню встановлена позначка про необхідність зміни паролю при першому вході в систему. Цю позначку можна зняти. Є і ніші позначки, які можна встановити («користувач не може змінити пароль», «термін дії паролю не обмежений», «відключити обліковий запис»)

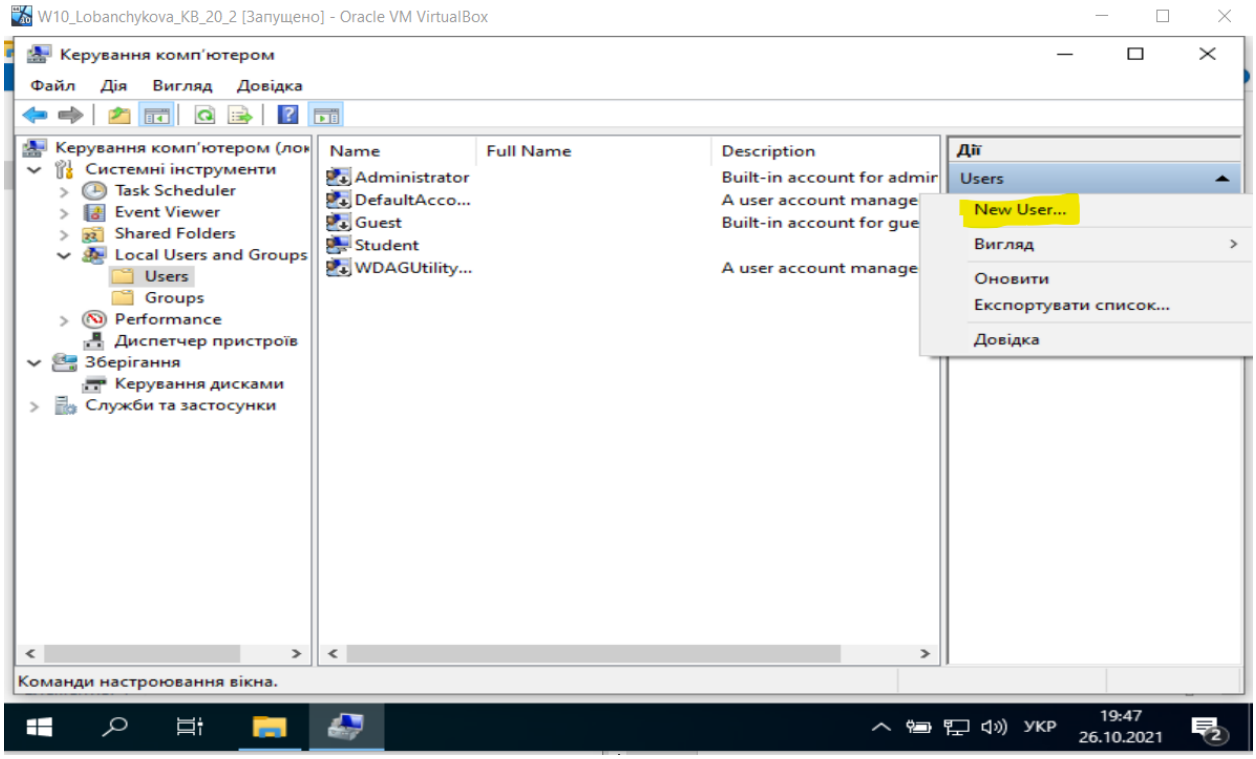

Рис.8 – Вікно для створення «Нового користувача»

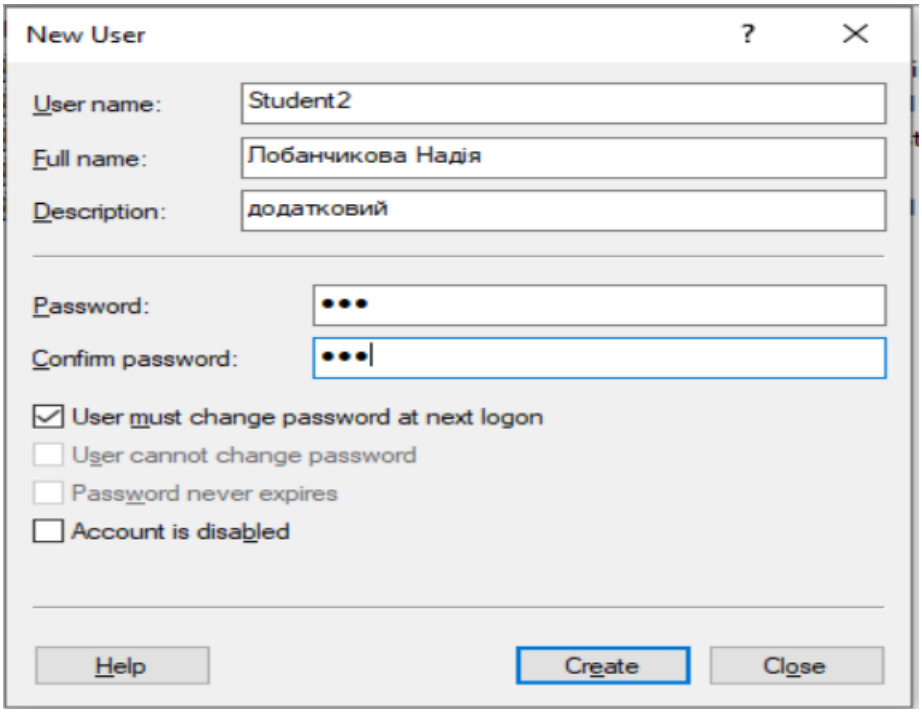

Рис.9 – Вікно введення параметрів користувача

За потреби встановлення програмного забезпечення при вході в систему під новостворeним користувачем, рис. 10, використовуйте функцію "Запуск от имени»". Натисніть клавішу Shift (праву кнопку миші) і виберіть "Запуск від імені іншого користувача", рисунок 11.

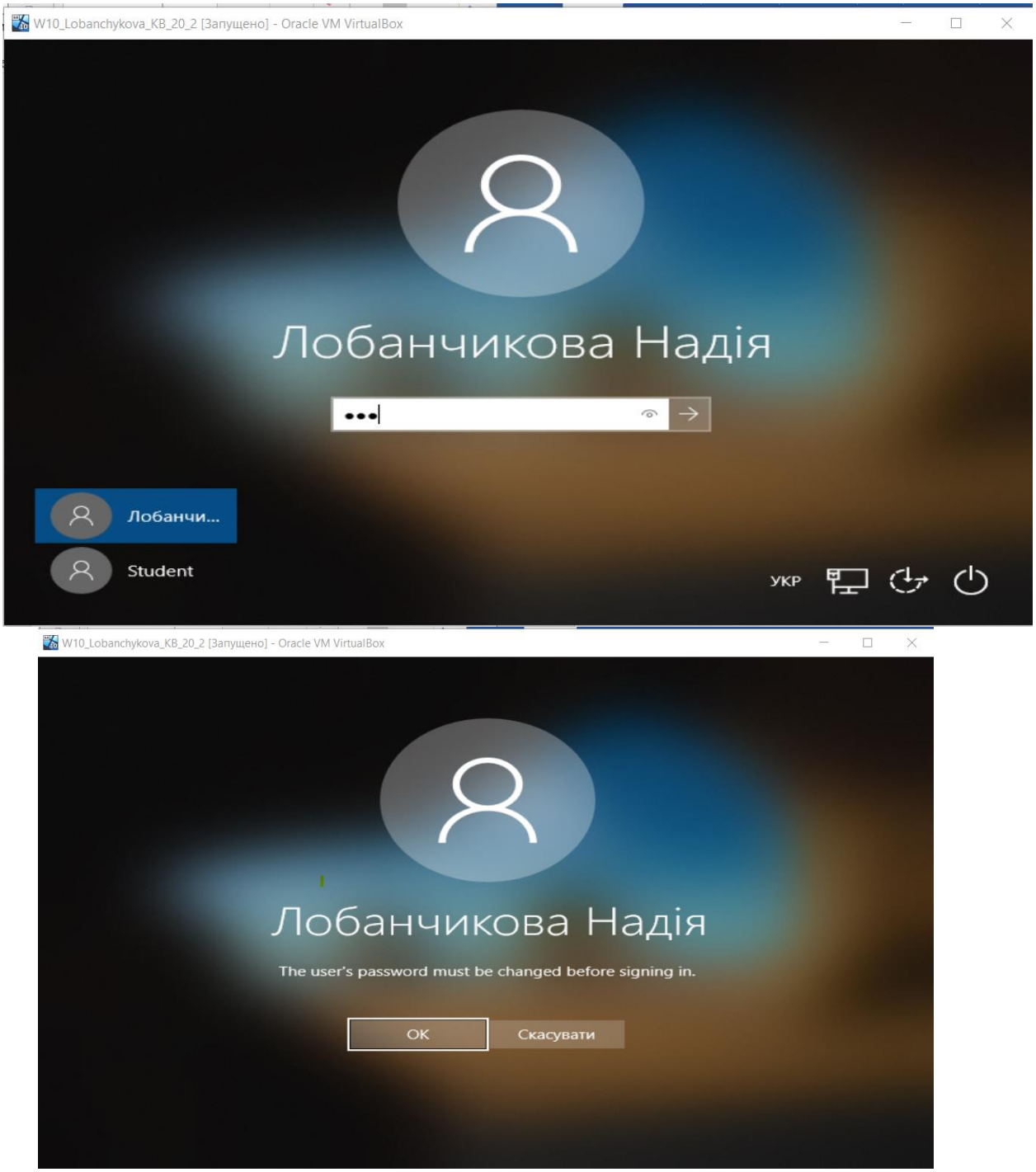

Рис.10 – Вхід ОС під новим користувачем

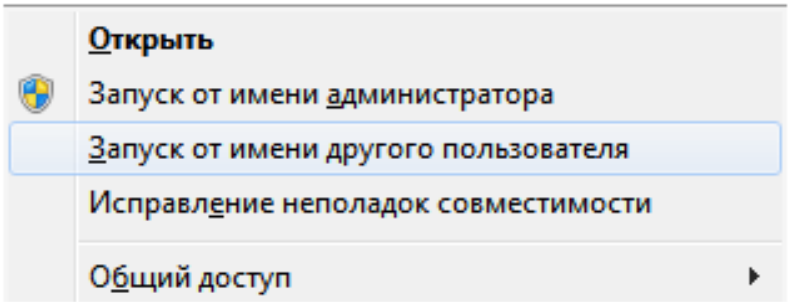

Рисунок 11.

Важливим кроком у справі захисту ваших паролів буде відключити шифрування на LMHash. Вимкнення виконується через політику локальної безпеки або в реєстрі. В другому випадку необхідно відкрити редактор реєстру: пошук → Виконати → **regedit.exe,** рис. 12.

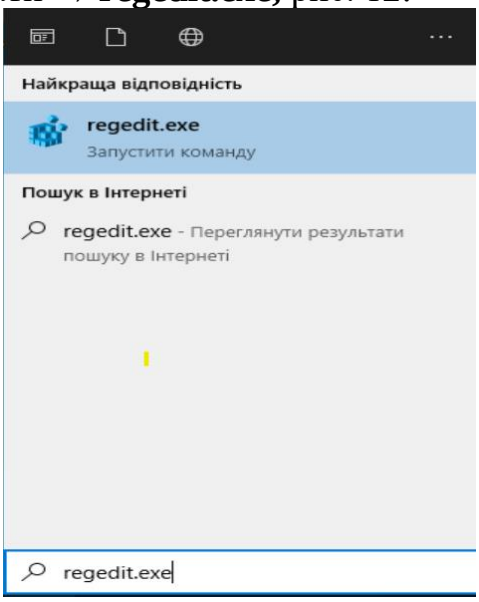

Рис.12 – знайдення та запуск реєстру

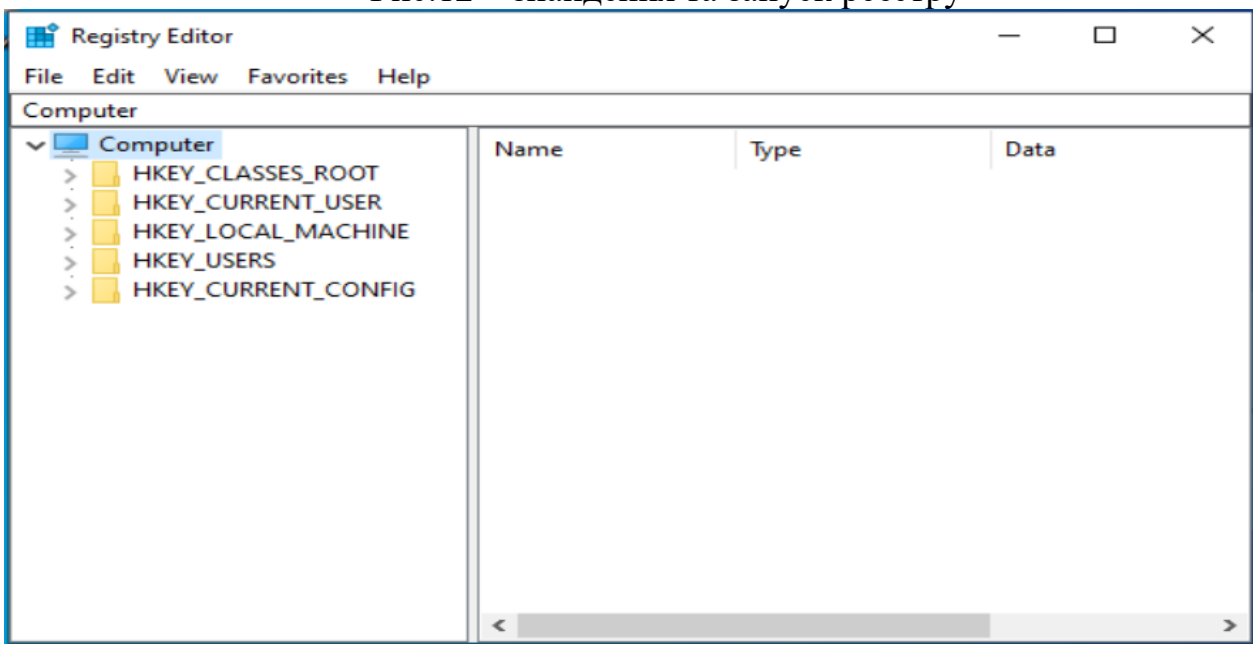

Рис. 13 – Вікно редактора реєстру

Знайти вітку:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

і перевірити параметр "NoLMHash" типу DWORD значення з значення даних 1.

Примітка: починаючи з Windows 7 SP1 у цього параметра вже встановлено по замовчуванню 1. У попередніх системах, або відсутній або дорівнює 0. Тому там необхідно було створювати його в ручному режимі.

1.4. Служби

В оснастці «Керування» шукаємо вкладку «Служби та застосунки», рисунок 15. Варто відзначити, що будь-яких служб дуже багато, але розглянемо найбільш популярні серед користувачів інтернету служби, видалення який забезпечить прискорення. Після того, як перед вами відкриється весь список служб можна натиснути на будь-який і в розділі «Властивості», «Тип запуску» встановити бажане значення. За допомогою цього ж меню можна просто провести відключення чи призупинити будь-яку службу в даний момент. Двічі клікнувши на будь-яку службу, можна зупинити або включити її, а також вибрати тип запуску: автоматичний – при включенні комп'ютера, вручну – за необхідності, відключено завантаження заборонена, служба не запускається, рис.14.

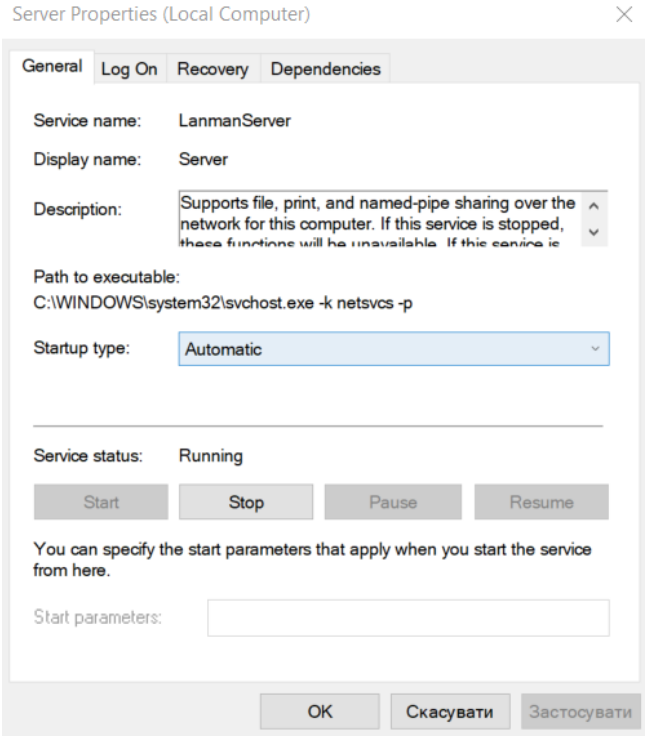

Рис.14

Крім цього, відключення здійснюється з використанням командного рядка (від Адміністратора), в яку вводиться sc config «Ім'я_служби» start=disabled. Всі дані для цієї команди знаходяться у верхній частині вікна при візуалізації відомостей про службу.

Далі проводимо відключення служб, які ми не використовуємо та тих служб, що нам не потрібні:

Microsoft Compatibility Telemetry. Служба, яка містить технічні дані про роботу пристрою і пов'язаного з ним програмного забезпечення. Вона періодично відправляє дані в Microsoft для подальшого поліпшення системи і підвищення зручності роботи користувачів. В цілому це важлива служба, але відключити її можна і нічого страшного з комп'ютером не відбудеться. Зупинити її роботу і прибрати компоненти можна в тому ж меню всіх сервісів, способом, описаним вище.

Windows Aero. Це графічна служба для красивого прозорого інтерфейсу. В цілому вона не потрібна і досить добре навантажує комп'ютер. Коли вона відключається, інтерфейс, зовнішній вигляд вікон і панелі завдань істотно може змінитися, але пристрій працювати стане краще.

Також до сервісів, що навантажує пристрій можна віднести Медіа центр Віндовс (Windows Media Center). Відключивши чи видаливши його, можна домогтися найкращої швидкодії - максимальної швидкості завантаження ОС (навіть до 10 сек). Така оптимізація доступна в двох варіантах: з допомогою видалення назовсім і відключення з можливістю відновлення в майбутньому. Але, щоб відключити цей центр потрібно буде звернутися до реєстру regedit.exe і видаляти певні ключі.

- Автономні файли - на домашньому ПК не використовуються.
- Браузер комп'ютерів - якщо у вас немає робочої групи, то відключіть.
- Сервер – не потрібен на машинах, які не виділяються ресурси для спільний доступу у мережі.
- Прослуховувач домашньої групи – залежить від служби "Сервер" зупиниться при її відключенні.
- Віддалений реєстр – безумовно відключити, оскільки віддалений доступ до нього вдома не потрібен.

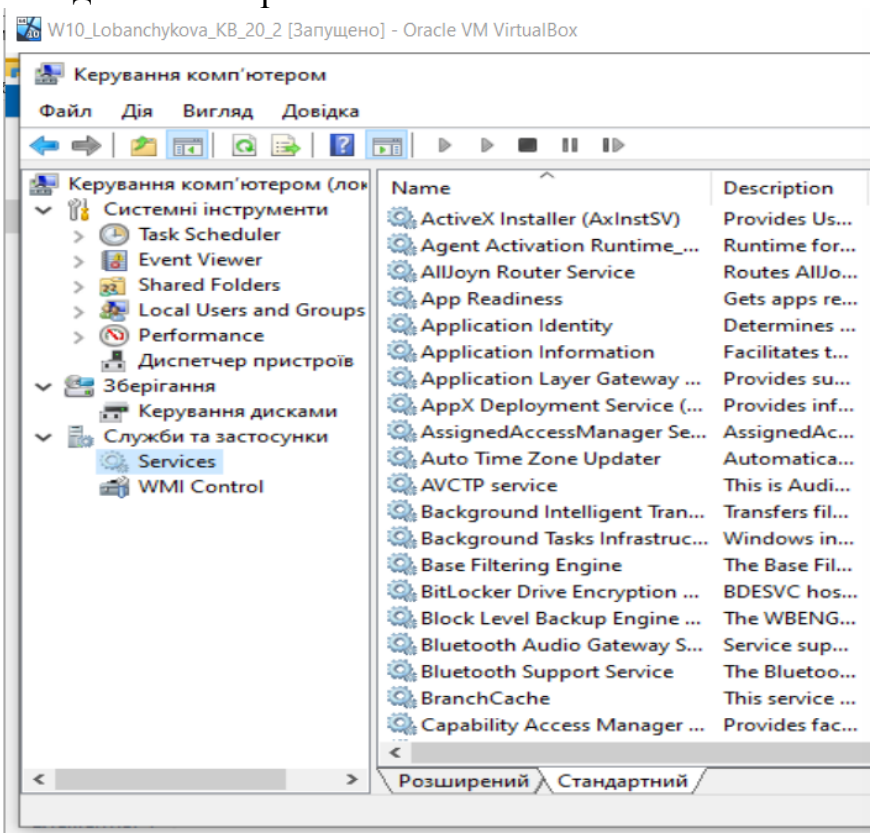

Рис. 15 – Вікно «Служби» керування комп’ютером

1.5. Локальні політики

Переходимо до налаштувань локальних політик безпеки. Для відкриття локальної політики безпеки необхідно запустити secpol.msc (можна задати через пошук та запустити), рис. 16

«Встановлюємо наступні значення, рис.17:
Політики облікових записів.

- Політика паролів – Мінімальна довжина пароля становить 10 символів.

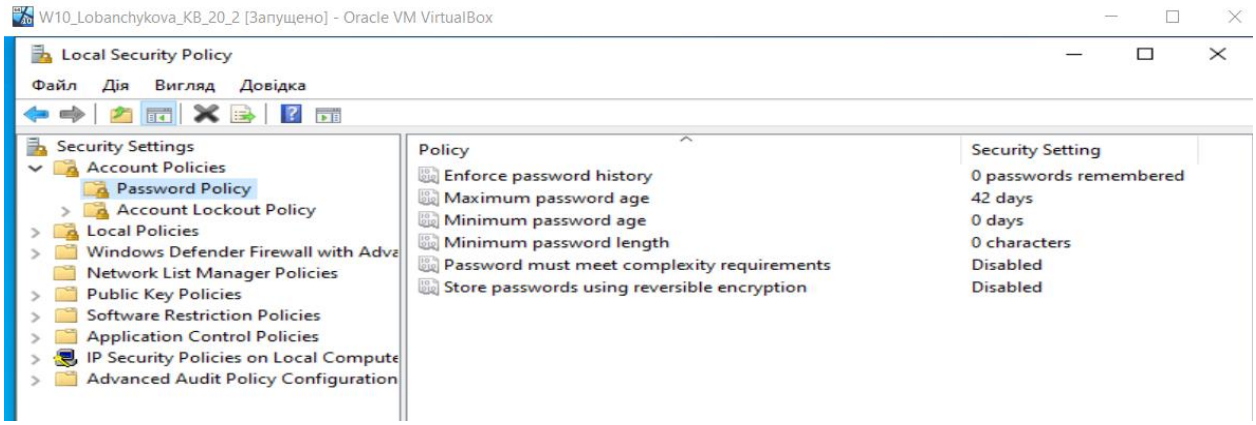

Рис.17 – Встановлення параметрів політики паролю

- Політика блокування облікових записів – порогове значення блокування 5 спроб на 10 хвилин, рис.18.

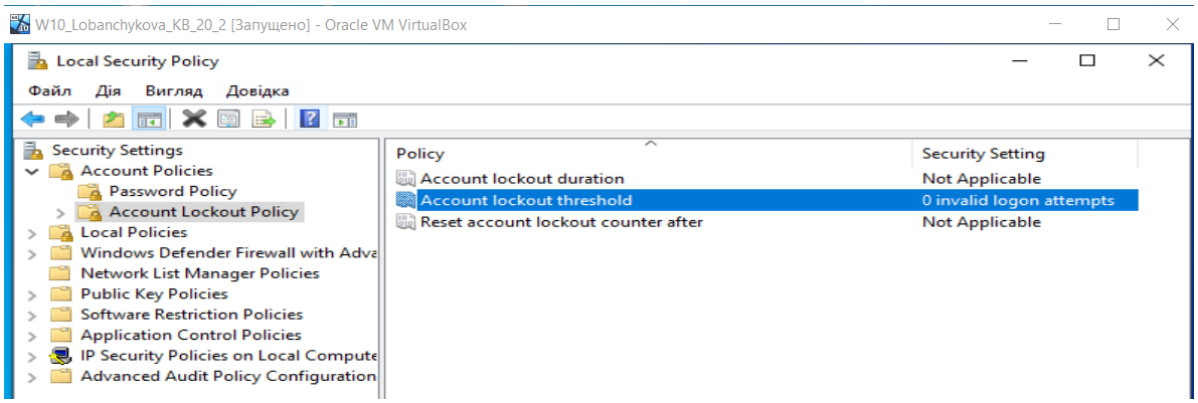

Рис. 18 – Встановлення параметрів блокування облікових записів

Локальні політики.

- Політика аудиту – Аудит входу в систему – Успіх та Відмова, рис. 19.

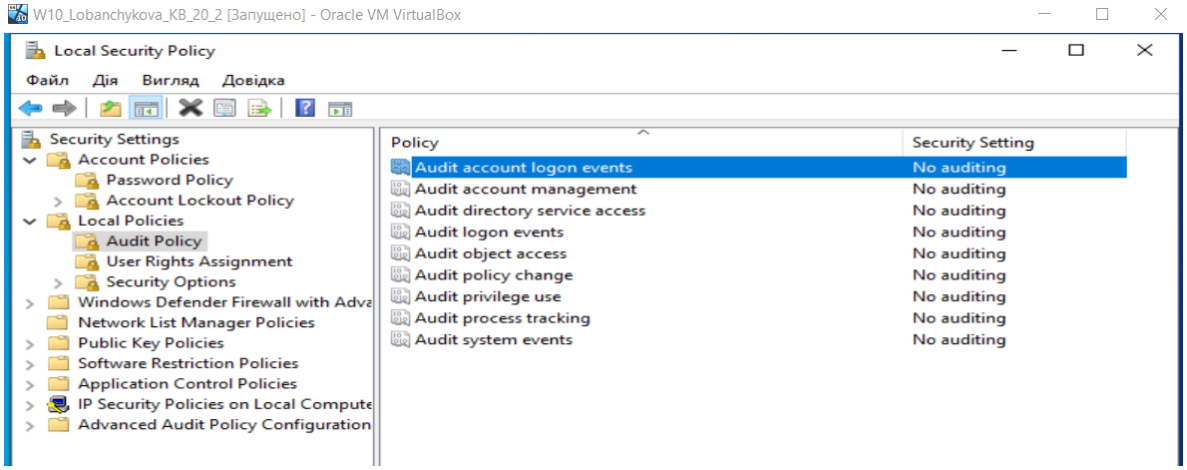

Рис. 19 – Встановлення параметрів аудиту входів у систему

- Політика аудиту – Аудит зміни політики – Успіх та Відмова, рис.20.

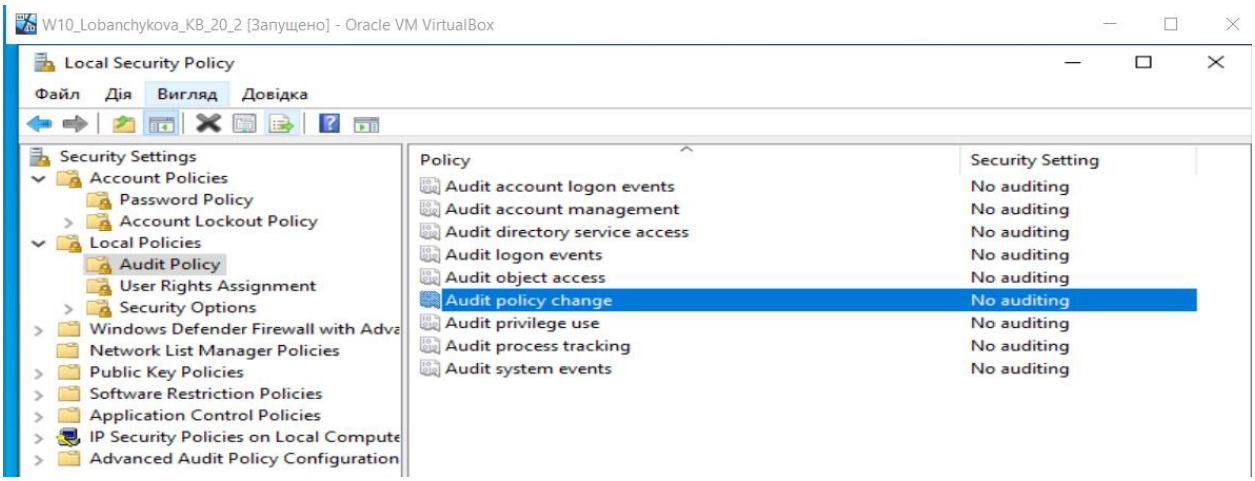

Рис. 20 – Встановлення параметрів аудиту зміни політики

- Політика аудиту – Аудит подій входу в систему – Успіх та Відмова, рис.21.

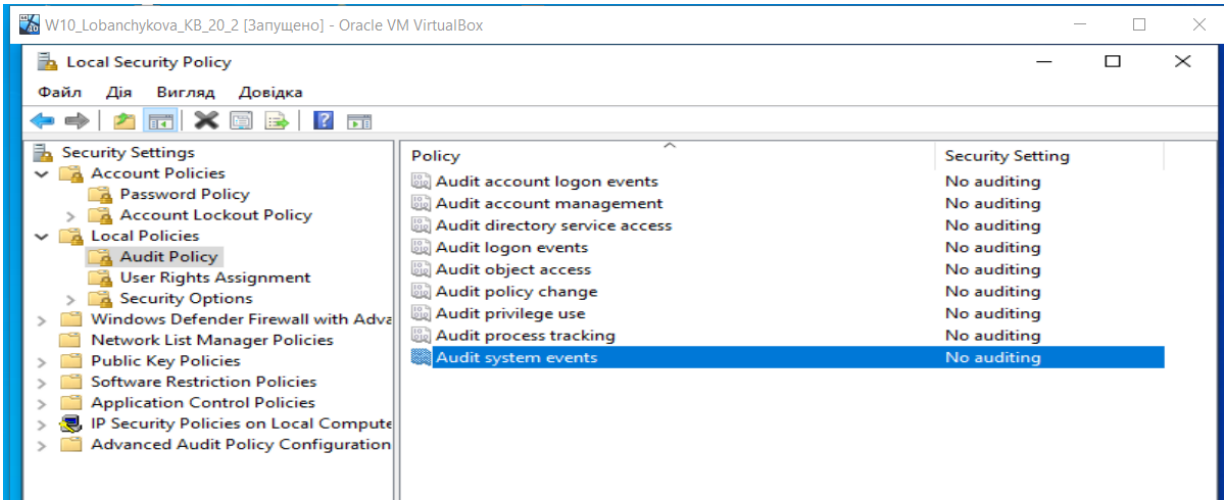

Рис.21 – Аудит подій входу у систему

- Призначення прав користувача – Доступ до комп'ютера з мережі, рис.12. Проаналізувати потрібність всіх зазначених користувачів. Залишити тільки тих, кому дійсно можна дозволити доступ.

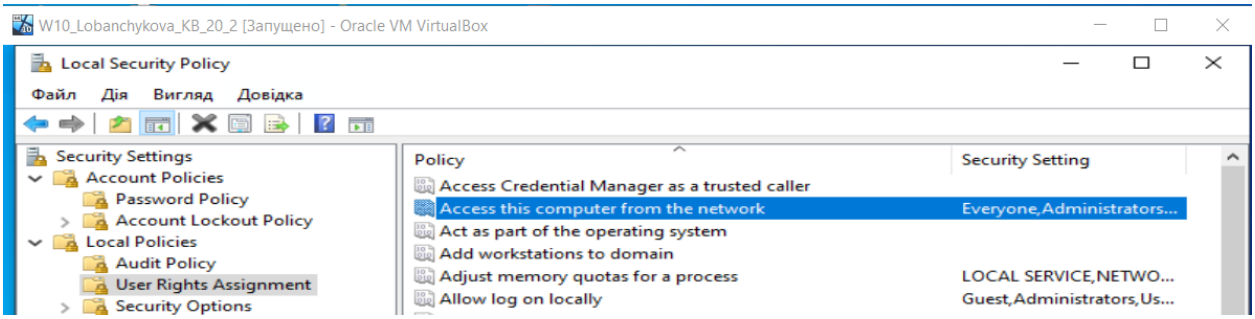

Рис. 22

- Призначення прав користувача – Локальний вхід в систему – Видалити "Гість".

- Параметри безпеки – Облікові записи: перейменування облікового запису адміністратора – вказати нове ім'я (прізвище студента), рис.23.

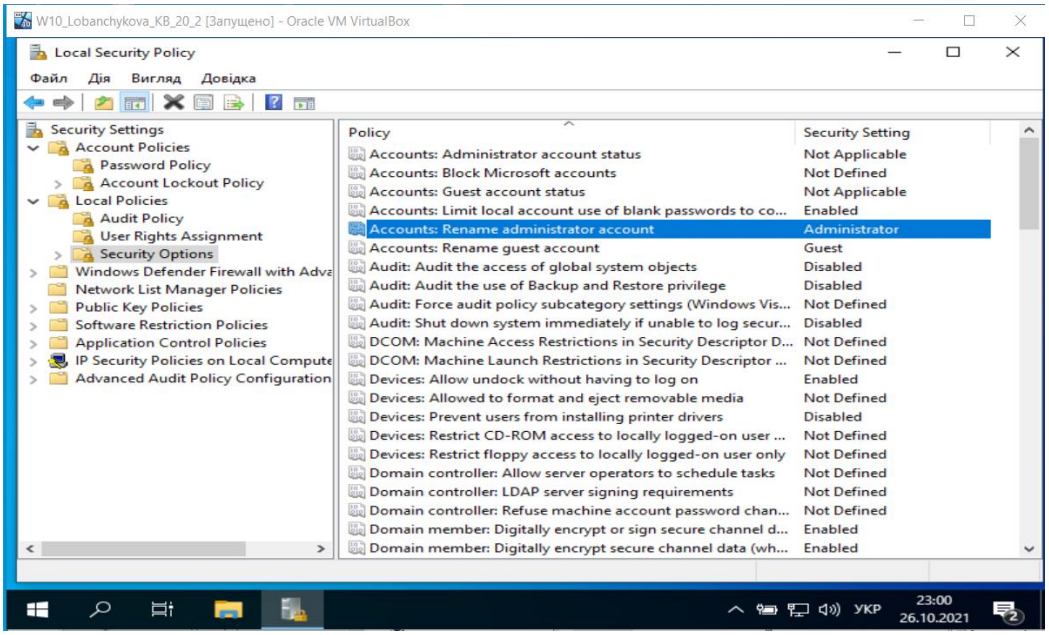

Рис. 23

- Параметри безпеки – Облікові записи: перейменування облікового запису гостя: вкажіть нове ім'я (скорочене прізвище студента).

- Параметри безпеки – Облікові записи: дозволити використання пустих паролів для входу тільки при консольному вході – Виключити.

- Безпека мережі: не зберігати хеш LAN Manager при наступній зміні пароля – Включено (увімкнуто),

P.S. вище зазначені параметри є достатніми для забезпечення безпечної експлуатації вашого комп'ютера.

Правила

1. Встановлюйте постійно оновлення.
2. Не використовуйте без необхідності обліковий запис «Адміністратор».
3. Не завантажувати програмне забезпечення із невідомих джерел. Намагайтеся завантажувати програмне забезпечення лише з сайту виробника.
4. Завантажуючи кряки і т. д. не забувайте про те, що таке програмне забезпечення може закінчиться негативно для вашого комп'ютера.
5. Виконуйте резервне копіювання даних.

ЗАВДАННЯ ДО ВИКОНАННЯ

1. Встановити оновлення та антивірусне програмне забезпечення на віртуальну машину з ОС Windows 10.

2. Створити 5 облікових записів за зразком Прізвище студента_N, де N – номер користувача (1,2,3,4,5).
3. Створити 2 групи користувачів за зразком Група_Р_К, де Р -порядковий номер студента у списку групи, К – порядковий номмер групи (1,2).
4. Задати паролі для входу кожного користувача та змінити їх при першому вході в систему. Використання складного паролю (числа + букви спеціальних символів, принаймні 10 символів у довжину, але в ідеалі 15-16).
5. Провести налаштування служб у відповідності до п.1.4.
6. Провести дослідження налаштувань локальних політик безпеки відповідно до п.1.5.
7. Оформити звіт та зробити висновки.

КОНТРОЛЬНІ ПИТАННЯ

1. Для чого використовується «Родина та інші користувачі»?
2. Яку максимальну кількість користувачів можна зареєструвати в ОС Windows 10 ?
3. Яким чином можна визначити стійкість паролю до зламу?
4. Рекомендовані вимоги до логіну та паролю.
5. Диспетчер задач та його призначення.

ЗМІСТ ЗВІТУ.

1. Назва, мета й завдання.
2. Опис дій в ході виконання роботи підтверджений відповідними рисунками (скріншотами). При формуванні звіту скріншоти виконання завдання повинні містити назву віртуальної машини.
3. Висновки про виконану роботу.