МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем та мереж»

Група: 4ФКС-56

Дипломний проект

здобувача освіти денної форми навчання
ФКС.56.03.000.ДП

Биховського Марка Віталійовича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Обслуговування комп'ютерних систем та мереж»**

Група: **4ФКС-56**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка та реалізація локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows

Проектний матеріал складається з пояснювальної записки на 104 сторінках та графічного (презентаційного) матеріалу на 10 аркушах (слайдах).

Дипломник_____(Биховський Марк.)

Керівни_____(Шевцов Ю.С.)

Консультанти:

з економічної части_____(Копайгородська Т.Г.)

з охорони праці_____(Чорновол Н.І.)

з дотримання вимог ЄСКД_____(Петрашова В.І.)

старший консультант_____(Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії_____(Кривченко Ю.В.)

Завідувач відділення_____(Скорнякова О.В.)

Захист «21» червня 2023 р. Протокол ДКК № 3

Оцінка ДКК 3 (задовільно)

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Обслуговування комп'ютерних систем та мереж»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 2023р.

ЗАВДАННЯ

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти Биховський Марк Віталійович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): Розробка та реалізація локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows

затверджена наказом по коледжу від "**17**" **жовтня** 2022 р. № **235-А2-ОД**

2. Термін здачі закінченого проекту (роботи) 12.06.2023

3. Вихідні данні до проекту (роботи): Забезпечення безпеки ресурсів за допомогою дозволів файлової системи NTFS,Аудит ресурсів і подій системи захисту Windows 10, Аудит об'єктів Windows 10,Створення базової конфігурації безпеки Windows 10

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Аудит та моніторинг; Файлова система NTFS ;Планування та встановлення дозволів NTFS; Зміна дозволів NTFS; Аудит ресурсів і подій системи захисту Windows 10; Налаштування політики аудиту; Налаштування аудиту об'єктів Windows 10; Керування журналом безпеки ;Засоби для базової конфігурації політики безпеки Windows 10;Економічна частина; Охорона праці

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Аудит та моніторинг; Вікно Додаткових параметрів безпеки для папки Public; Вікно запису дозволів для папки Public; Повідомлення про недостатність прав для відкриття файлу WITHOUTACCESS; Вікно для вибора Користувачів або Групи; Вікно Додаткові параметри безпеки для Owner; Вікно з властивостями файла OWNER; Змінення дозволів для користувача Василій; Вже зміненний власник файлу Owner; Прибирання Спадкоємство від батьківського об'єкта для користувача Василій

6.Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Шевцов Ю.С.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7.Дата видачі завдання

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етаповдипломного проекту (роботи)	Відмітка про виконання
1.	Огляд літератури. Огляд існуючих рішень.	22.05.2023	Виконав
2.	Аналіз локальної політики безпеки комп'ютерної системи.	24.05.2023	Виконав
3.	Огляд методів захисту від шкідливих програм	29.05.2023	Виконав
4.	Огляд сервісів безпеки Windows 10	01.06.2023	Виконав
5.	Аналіз файлової системи NTFS	03.06.2023	Виконав
6.	Аналіз аудиту ресурсів і подій системи захисту Windows 10	05.06.2023	Виконав
7.	Дослідження керування журналом безпеки	07.06.2023	Виконав
8.	Розробра засобів політики безпеки Windows 10	09.06.2023	Виконав
9.	Підготовка до попереднього захисту, підготовка до захисту	11.06.2023	Виконав
10.	Отримання рецензії, відповіді на зауваження рецензента	15.06.2023	Виконав
11.	Захист роботи	19.06.2023	Виконав

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			ФКС.56.03.000.ДП	Дипломний проект	100	
А4			ФКС.56.03.000.ДП.ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	ФКС.56.03.000.ДП		
Розробив		Биховський М.В..			Розробка та реалізація локальної політики безпеки за допомогою сервісів Windows	Літ.	Аркуш 4 / Аркушів
Перевірив		Шевцов Ю.С.				У Д П	
Н. Контр.		Петрашова В.І.				ОТФК ОНТУ, гр. 4ФКС-56	
Затверд.		Кривченко Ю.В..					

ЗМІСТ

ВСТУП

У сучасному світі, де комп'ютерні системи відіграють вирішальну роль у кожному аспекті нашого життя, безпека комп'ютерних систем стає критично важливим завданням.

Запобігання таким загрозам, як віруси, хакерські атаки та розкриття конфіденційної інформації, є необхідною умовою для забезпечення безпеки та захисту комп'ютерних систем. Одним із важливих аспектів безпеки комп'ютерної системи є розробка та впровадження локальних політик безпеки.

Локальна політика безпеки Windows — це набір правил, параметрів і обмежень, які встановлюються на окремому комп'ютері під керуванням операційної системи Windows. Він визначає правила, що регулюють доступ до ресурсів комп'ютера, автентифікацію користувачів, захист від вірусів і шкідливих програм та інші аспекти безпеки.

Метою локальної політики безпеки Windows є забезпечення конфіденційності, цілісності та доступності даних, а також запобігання несанкціонованому доступу до системи та її ресурсів. Він визначає правила для користувачів, груп користувачів і самої операційної системи для забезпечення захисту від різних загроз і зловживань.

В рамках даної дипломної роботи буде проведено детальний аналіз локальної політики безпеки Windows, а також розроблено стратегії та рекомендації щодо її реалізації. Дослідження буде зосереджено на розумінні ключових принципів безпеки Windows.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Локальна політика безпеки комп’ютерної системи.

Операційна система Windows має низку оснасток і політик, які є елементами конфігурації для різних функціональних компонентів операційної системи. Однією з таких оснасток є Локальна політика безпеки ,яка відповідає за редагування механізмів безпеки Windows.

Локальна політика безпеки комп'ютерної системи включає в себе набір правил, настанов і процедур, які встановлюються на рівні окремої системи або комп'ютера для забезпечення безпеки. Ця політика призначена для захисту інформації, збереження цілісності системи та попередження несанкціонованого доступу до ресурсів.

Основні аспекти локальної політики безпеки комп'ютерної системи включають:

- Політика паролів
- Аутентифікація і авторизація
- Захист від шкідливих програм
- Керування правами доступу
- Аудит та моніторинг

1.1.1 Поняття політики паролів

Політика паролів - це набір правил і вимог, встановлених організацією або системним адміністратором для використання надійних і безпечних паролів. Політика розробляється для забезпечення безпеки інформації та запобігання несанкціонованому доступу до системи шляхом вгадування або перехоплення паролів. На рисунку Рис.1.1 зображено як виглядає діалогове вікно для зміни політики .

Основними поняттями, пов'язаними з політикою паролів, є

- Складність пароля: політика паролів встановлює вимоги до складності пароля.

  Це означає, що паролі мають містити різні типи символів, включно з великими та малими літерами, цифрами та спеціальними символами.

- Наприклад, потрібно використовувати щонайменше вісім символів, включно з буквами верхнього і нижнього регістру, цифрами і спеціальними символами.
- Мінімальна довжина пароля: політика паролів дає змогу встановити мінімальну довжину пароля, наприклад, мінімум вісім символів. Що довший пароль, то складніше його вгадати або дізнатися.
- Заборона на використання легко вгадуваних паролів: політика паролів може забороняти використання очевидних або легко вгадуваних паролів, таких як "123456", "пароль" або ім'я користувача. Вони також можуть включати механізми перевірки нових паролів за певним списком часто використовуваних або слабких паролів.
- Регулярна зміна паролів: політика паролів може вимагати регулярної зміни паролів. Це запобігає використанню одних і тих самих паролів упродовж тривалого періоду часу та знижує ризик уразливості через компрометацію пароля або здогадки.

Використання політик паролів є важливим аспектом безпеки комп'ютерних систем. Вона запобігає несанкціонованому доступу до інформації, зберігає конфіденційність і запобігає втраті даних. Ефективна політика паролів вимагає ретельного впровадження, контролю та навчання користувачів дотримання встановлених правил безпеки паролів.

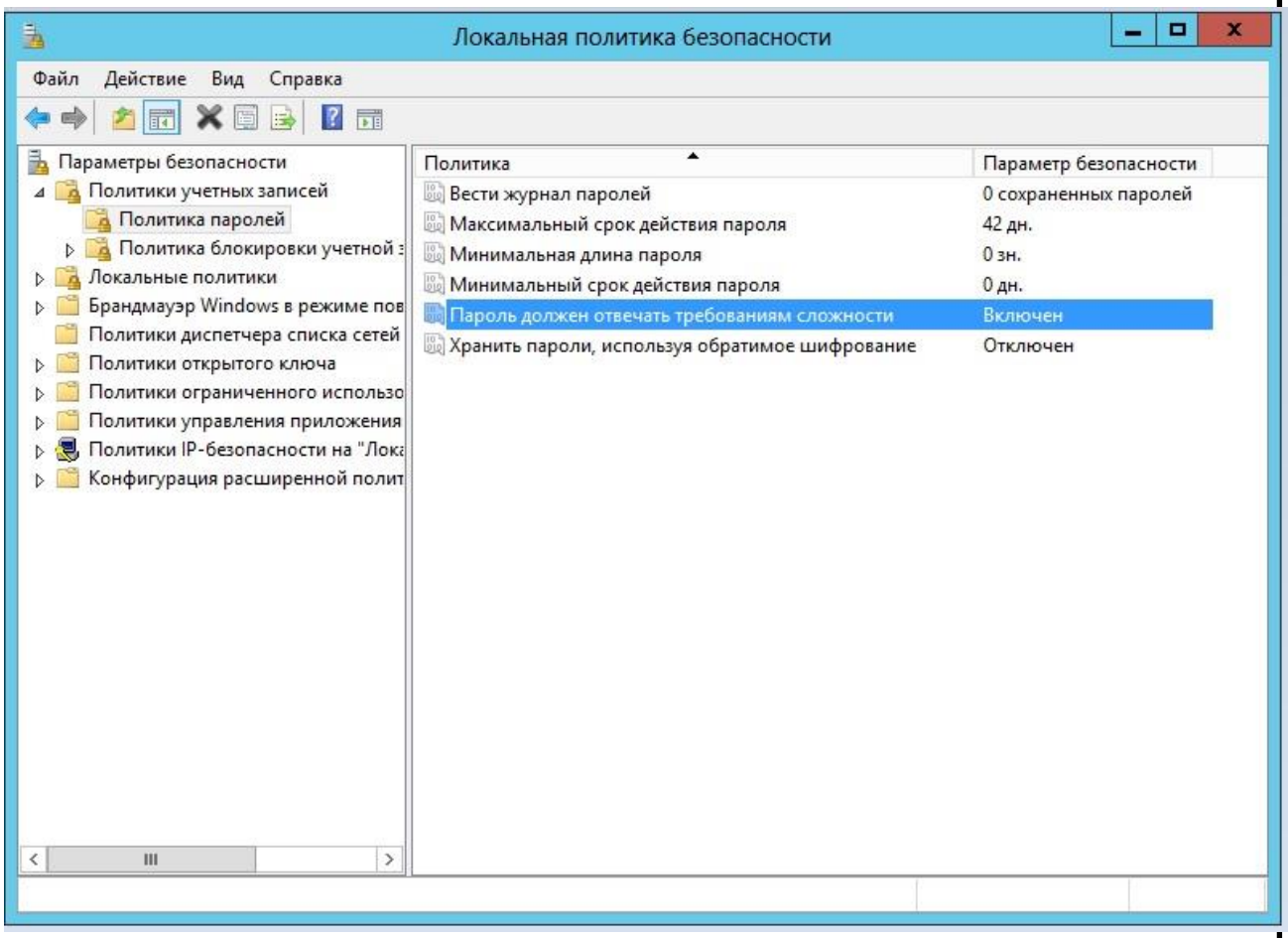


Рисунок 1.1- Діалогове вікно для зміни політики паролів

1.1.2 Поняття про безпеку аутентифікації та авторизації

Безпека аутентифікації та авторизації є важливим аспектом комп'ютерних мереж, оскільки вона визначає, хто може отримати доступ до ресурсів і які дії можуть виконувати ці користувачі. Приклад з автентифікацією можна побачити на Рис. 1.2

Давайте докладніше розглянемо кожне з цих понять:

- Автентифікація:

  Автентифікація: автентифікація - це процес перевірки особи користувача або пристрою, який намагається отримати доступ до

комп'ютерної мережі. Це робиться шляхом введення користувачем унікальних облікових даних, як-от ім'я користувача та пароль, або за допомогою біометричних методів, як-от сканування відбитків пальців або розпізнавання обличчя. Аутентифікація дає змогу перевірити особу Користувача або пристрою.

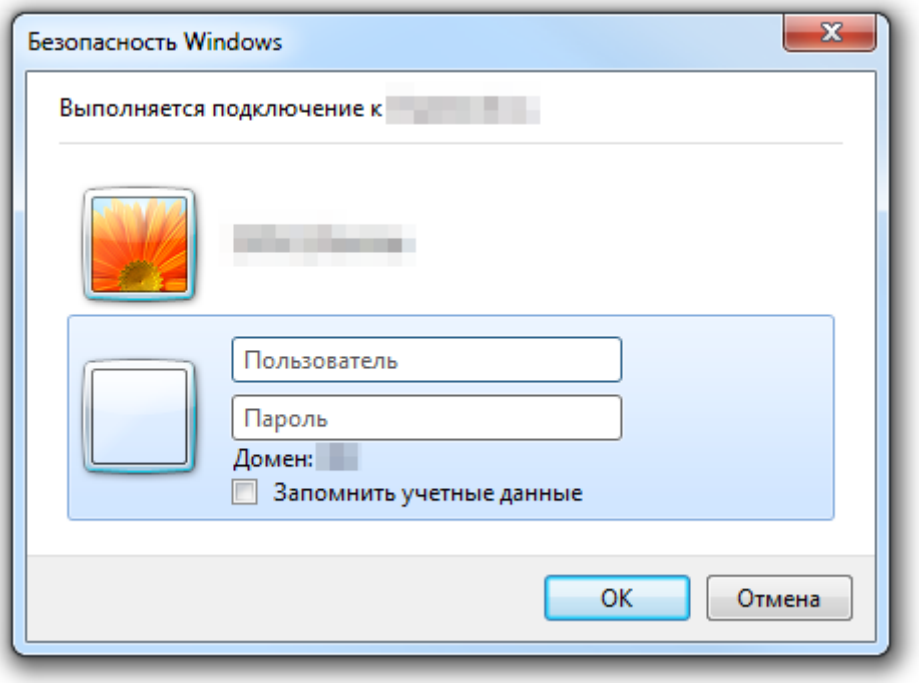


Рисунок 1.2 – Діалогове вікно для автентифікації користувача

- Авторизація :

  Авторизація - це процес надання прав доступу після успішної аутентифікації. Після аутентифікації користувача система перевіряє його особистість і визначає, які ресурси та функції він має право використовувати. Це може бути зроблено шляхом призначення ролей або груп користувачам з певними правами доступу до певних ресурсів. Авторизація контролює, хто може отримати доступ до ресурсів і які дії вони можуть виконувати.

Принципи безпеки аутентифікації та авторизації

Для забезпечення ефективної безпеки аутентифікації та авторизації в комп'ютерних мережах необхідно дотримуватися низки принципів:

- Надійна аутентифікаційна інформація: важливо використовувати надійні паролі та інші форми аутентифікаційної інформації, що складаються з комбінацій букв, цифр і спеціальних символів.
- Принцип мінімальних прав доступу: користувачам повинні надаватися тільки ті права доступу, які необхідні їм для виконання своїх обов'язків. Це знижує ризик несанкціонованого доступу до конфіденційної інформації.
- Аудит і моніторинг: важливо мати механізми для аудиту та моніторингу дій користувачів у системі. Це дає змогу виявити підозрілу або незвичайну активність, яка може вказувати на несанкціонований доступ або зловживання привілеями.
- Регулярне оновлення Важливо підтримувати програмне забезпечення та операційні системи в актуальному стані, оскільки вони часто випускають виправлення і доповнення для виявлених вразливостей. Це допомагає запобігти використанню вразливостей і доступу до них неавторизованих осіб.

Загалом, безпека автентифікації та авторизації в комп'ютерних системах важлива для захисту конфіденційності, цілісності та доступності даних. Використання надійних облікових даних, принципу найменшого доступу, аудиту та моніторингу, а також регулярне оновлення системи може допомогти підвищити безпеку мережі та знизити ризик несанкціонованого доступу.

1.1.3 Захист від шкідливих програм

Захист від шкідливого програмного забезпечення є важливим компонентом локальної політики безпеки комп'ютерної системи. Шкідливі програми, такі як віруси, хробаки, троянські коні та шпигунські програми, можуть пошкодити системи, вкрасти конфіденційні дані, пошкодити файлові системи, порушити конфіденційність і доступ до системи та сповільнити роботу систем.

Для ефективного захисту від шкідливих програм можна вжити таких заходів

- Встановити антивірусне програмне забезпечення: антивірусне програмне забезпечення допомагає виявляти, блокувати і видаляти шкідливі програми з вашої системи. Антивірусне ПЗ сканує файли, електронну пошту та веб-сторінки для виявлення вірусів та інших загроз.
- Регулярно оновлювати антивірусне програмне забезпечення: постійно з'являються нові шкідливі програми, тому важливо регулярно оновлювати антивірусне програмне забезпечення. Оновлення включають нові визначення вірусів і сигнатури для виявлення нових загроз.
- Використовування брандмауера: брандмауер - це програма або пристрій, який контролює надсилання та отримання мережевого трафіку. Блокуючи небажаний трафік і забороняючи несанкціоновані підключення, він може запобігти проникненню шкідливих програм до системи або виходу з неї.

- Навчання користувачів Навчання користувачів загрозам і заходам безпеки є не менш важливою частиною захисту від шкідливого ПЗ. Користувачі повинні знати про ризики, пов'язані із завантаженням заражених файлів, відкриттям неперевірених електронних листів, переходом за посиланнями невідомого походження тощо.

Ці заходи допомагають ефективно захиститися від шкідливого ПЗ і знизити ризик інцидентів, пов'язаних із безпекою комп'ютерних систем. Важливо регулярно переглядати й оновлювати політику безпеки з урахуванням останніх тенденцій і загроз, а також проводити аудити безпеки для виявлення потенційних слабких місць і вразливостей.

1.1.4 Управління правами доступу

Управління правами доступу (ARM) є важливим компонентом локальної політики безпеки для комп'ютерних систем. Це процес налаштування, контролю та управління правами доступу користувачів до різних ресурсів, включно з файлами, папками, додатками, мережами та базами даних. Управління правами доступу допомагає обмежити доступ до конфіденційної інформації, запобігти несанкціонованій модифікації даних і забезпечити цілісність системи.

Основними аспектами управління правами доступу є

- Ідентифікація та автентифікація користувачів: ідентифікація та автентифікація користувачів: це перший крок у процесі управління правами доступу. Кожен користувач має бути ідентифікований унікальним ім'ям або ідентифікатором і повинен пройти процес автентифікації для підтвердження своєї особи, наприклад, ввести пароль або використовувати біометричні дані.
- Налаштування ролей і груп доступу: ролі та групи доступу допомагають організувати користувачів відповідно до їхніх функціональних обов'язків і рівня доступу до ресурсів. Кожна роль або група може мати

свій власний набір прав доступу, що дає змогу адміністраторам легко керувати доступом до ресурсів для багатьох користувачів одночасно.

- Надання привілеїв: привілеї можуть використовуватися для виконання певних дій або підвищення рівня доступу. Системні адміністратори можуть надавати привілеї окремим користувачам або ролям залежно від їхніх вимог та обов'язків.

  Наприклад, системний адміністратор може мати право доступу до всіх ресурсів і право змінювати системні налаштування.
- Встановлення обмежень доступу: управління правами доступу також включає в себе встановлення обмежень для певних користувачів або ролей. Це включає обмеження доступу до певних ресурсів, заборону певних операцій, обмеження права на зміну системних налаштувань тощо.
- Аудит і моніторинг: управління правами доступу вимагає наявності механізмів аудиту та моніторингу для відстеження активності користувачів. Це дає змогу виявити підозрілу активність, спроби несанкціонованого доступу та втручання в роботу системи.
- Регулярне оновлення політик: політики управління правами доступу повинні переглядатися й оновлюватися на регулярній основі. Це може включати зміну прав доступу користувачів і ролей, встановлення нових обмежень і дозволів, а також аналіз поточних загроз і врахування нових технологій і тенденцій у сфері безпеки.

Ефективне управління правами доступу допомагає забезпечити принципнайменших привілеїв (безпеки), за якого користувачам надається тільки той рівень прав доступу, який необхідний для виконання їхніх завдань. Це знижує ризик несанкціонованого доступу, витоку інформації та інших загроз безпеці системи.

1.1.5 Аудит та моніторинг

Аудит та моніторинг є важливою складовою локальної політики безпеки комп'ютерної системи. Вони допомагають виявляти, аналізувати та реагувати на події, що відбуваються в системі з метою забезпечення безпеки та виявлення потенційних загроз.

Аудит означає систематичне переглядання та оцінку активності, подій і реєстрації в системі. Основна мета аудиту - забезпечення достатнього контролю, перевірка виконання політики безпеки, виявлення несправностей, вразливостей і виявлення аномальної діяльності. В ході аудиту можуть бути перевірені журнали подій, системні журнали, журнали доступу до файлів та інші системні ресурси.

Моніторинг, з свого боку, є процесом постійного спостереження за системою з метою виявлення потенційних загроз і вразливостей. Моніторинг може включати перевірку системних ресурсів, мережевої активності, шаблонів поведінки користувачів, аналіз забезпечення безпеки, детектування вторгнень і виявлення аномальних змін у системі.

Основні аспекти аудиту та моніторингу включають:

- Журналювання подій: Запис подій в системні журнали є важливим елементом аудиту та моніторингу. Це включає реєстрацію дій користувачів, доступ до ресурсів, зміни налаштувань системи та інші події, які можуть мати вплив на безпеку системи. Журнали дозволяють адміністраторам аналізувати активність, виявляти вразливості та спроби несанкціонованого доступу.
- Аналіз журналів подій: Після збору журналів подій важливо провести їх аналіз з метою виявлення потенційних загроз та аномальної діяльності.

- Це може включати пошук підозрілих шаблонів, спостереження за змінами в активності, виявлення незвичайних дій користувачів та інших ознак можливої загрози.
- Вторгнення та вразливості: Аудит та моніторинг також спрямовані на виявлення вторгнень і вразливостей системи. Це може включати сканування мережі на наявність вразливих точок, аналіз журналів з метою виявлення підозрілих дій, використання системи детектування вторгнень (IDS) і системи запобігання вторгнень (IPS) для спостереження за мережевою активністю.
- Реагування та відновлення: Важливо мати плани реагування на інциденти та відновлення після них. Аудит та моніторинг допомагають виявляти загрози та несправності, що вимагають негайних заходів забезпечення безпеки. Це може включати блокування доступу, зміну паролів, відновлення системи з резервних копій та інші заходи для відновлення нормального функціонування системи.

Аудит та моніторинг є важливими інструментами для виявлення загроз, захисту від інцидентів безпеки та забезпечення безпеки комп'ютерної системи. Правильно налаштовані процеси аудиту та моніторингу допомагають попереджати можливі атаки, виявляти вразливості та швидко реагувати на них для забезпечення безпеки і цілісності системи.

1.1.6 Сервіси безпеки Windows

Windows надає різноманітні сервіси безпеки, які допомагають забезпечити захист комп'ютерної системи.Основні сервіси безпеки, доступні в операційній системі Windows, включають наступні:

- Windows Defender
- Фаєрвол Windows
- Windows BitLocker

- Windows Update
- Підписи драйверів Windows
- SmartScreen

1.1.7 **Windows Defender**

Windows Defender є вбудованим антивірусним програмним засобом в операційній системі Windows. Він призначений для захисту комп'ютера від різних видів загроз, таких як віруси, шпигунське програмне забезпечення, троянські програми та інші шкідливі програми. Він має простий інтерфейс який можна побачити на Рис. 1.3

Ось деякі особливості та функції Windows Defender:

- Антивірусний движок: Windows Defender включає потужний антивірусний двигун, який виявляє та блокує відомі віруси і шкідливі програми. Він постійно оновлюється через Windows Update, щоб забезпечити останні бази даних вірусних визначень.
- Захист в реальному часі: Windows Defender працює в фоновому режимі, постійно моніторить активність системи та виявляє шкідливі програми під час їх запуску або виконання. Він автоматично реагує на потенційні загрози та вживає заходів для їх блокування.
- Захист від розширень браузера: Windows Defender включає розширення для популярних веб-браузерів, таких як Microsoft Edge та Google Chrome. Ці розширення допомагають виявляти і блокувати шкідливі веб-сайти, фішингові атаки та інші загрози в реальному часі.
- Захист від розповсюдження шкідливого ПЗ: Windows Defender включає захист від виконання шкідливих файлів, що запобігає їх виконанню або встановленню на комп'ютер без дозволу користувача. Це допомагає

забезпечити безпеку системи від шкідливих програм, які можуть пошкодити файли або викрасти конфіденційну інформацію.

- Інтеграція з іншими захистними функціями: Windows Defender інтегрований з іншими сервісами безпеки, такими як Фаєрвол Windows і Захист від загроз Microsoft. Це забезпечує комплексний підхід до захисту системи від різних видів загроз.Крім того, Windows Defender дозволяє проводити повні, швидкі або вибіркові сканування системи для виявлення і видалення загроз.

Windows Defender є потужним і ефективним інструментом безпеки, який забезпечує базовий рівень захисту комп'ютера від шкідливих програм.

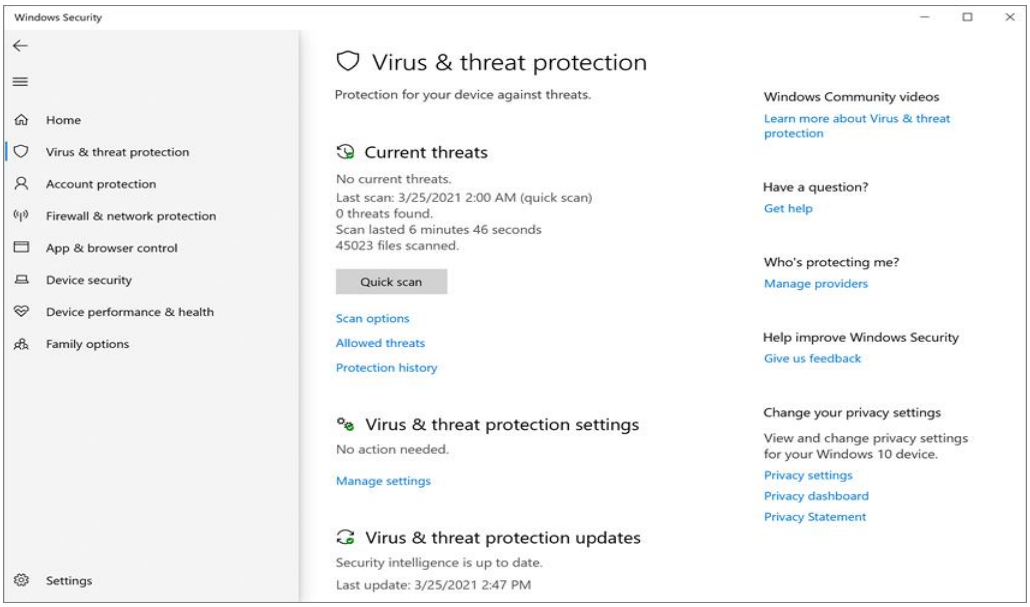


Рисунок 1.3 Панель керування Windows Defender.

1.1.8 **Фаєрвол Windows**

Фаєрвол Windows є вбудованим механізмом безпеки в операційній системі Windows. Він працює на рівні мережі та дозволяє контролювати трафік, який входить і виходить з вашої комп'ютерної системи.

Ось деякі ключові аспекти та функції Фаєрволу Windows:

- Фільтрація мережевого трафіку: Фаєрвол Windows аналізує всі мережеві пакети, які надходять до вашого комп'ютера або надсилаються з нього. Він застосовує набір правил та політик, щоб вирішувати, які з'єднання мають бути дозволені або заборонені. Це дозволяє блокувати небажаний або потенційно небезпечний трафік.
- Блокування несанкціонованого доступу: Фаєрвол Windows допомагає захистити ваш комп'ютер від несанкціонованого доступу зовнішніми мережами. Він може блокувати з'єднання, які намагаються проникнути в вашу систему через вразливості або небезпечні порти. Ви можете налаштувати Фаєрвол таким чином, щоб він дозволяв тільки деякі типи з'єднань або ресурсів.
- Управління правилами: Фаєрвол Windows дозволяє налаштовувати правила фільтрації трафіку в залежності від вашого потреби. Ви можете встановлювати правила на основі IP-адрес, портів, протоколів тощо. Наприклад, ви можете дозволити з'єднання до певного порту для певної програми або блокувати доступ з певних IP-адрес.
- Захист від фішингу та інших загроз: Фаєрвол Windows може включати додаткові функції безпеки, такі як захист від фішингу. Він може виявляти та блокувати небезпечні веб-сайти або веб-посилання, які намагаються обманути вас та отримати вашу конфіденційну інформацію.
- Інтеграція з іншими інструментами безпеки: Фаєрвол Windows може працювати спільно з іншими сервісами безпеки, такими як Windows Defender або антивірусним програмним забезпеченням сторонніх виробників. Це забезпечує комплексний захист комп'ютерної системи від різних видів загроз.

Фаєрвол Windows є важливою складовою локальної політики безпеки комп'ютерної системи. Він допомагає забезпечити безпеку мережі, захистити ваші дані та пристрої від небажаних підключень та загроз зовнішніх мереж.

1.1.9 **Windows BitLocker**

Windows BitLocker є вбудованим рішенням шифрування диска, доступним у операційній системі Windows. Він призначений для захисту даних на комп'ютері шляхом шифрування всього диску або окремих розділів.

Ось деякі основні аспекти та функції Windows BitLocker:

- Шифрування даних: Windows BitLocker використовує сильне шифрування, щоб захистити дані на вашому диску. Він використовує алгоритми шифрування, такі як Advanced Encryption Standard (AES), для забезпечення високого рівня безпеки. Після шифрування диску дані залишаються незрозумілими для несанкціонованих користувачів, які не мають відповідного ключа або пароля.
- Шифрування всього диску або окремих розділів: Windows BitLocker дозволяє шифрувати всій диск або окремі розділи на диску. Ви можете вибрати, які розділи шифрувати залежно від вашої потреби. Це дозволяє вам захистити конфіденційні дані, залишаючи інші розділи доступними без необхідності вводу пароля.
- Режими шифрування: Windows BitLocker пропонує два режими шифрування - режим шифрування диску і режим шифрування USB-носія. Режим шифрування диску призначений для захисту даних на внутрішньому диску комп'ютера, тоді як режим шифрування USB-носія дозволяє шифрувати дані на зовнішніх пристроях зберігання, таких як флеш-накопичувачі або зовнішні жорсткі диски.

- Керування ключами шифрування: Windows BitLocker автоматично генерує ключ шифрування для кожного зашифрованого диску або розділу. Цей ключ може бути збережений на локальному комп'ютері або в режимі Active Directory. Ви також можете налаштувати використання додаткових методів авторизації, таких як пароль, PIN-код або USB-ключ, для доступу до зашифрованих даних.
- Інтеграція з платформою TPM: Trusted Platform Module (TPM) - це апаратний компонент, який може бути вбудований в деякі комп'ютери. Windows BitLocker може використовувати TPM для забезпечення додаткової безпеки. TPM може зберігати ключ шифрування та гарантувати, що диск не може бути розшифрований на іншому комп'ютері.

Windows BitLocker є потужним інструментом шифрування, який допомагає забезпечити безпеку даних на вашому комп'ютері або зовнішніх пристроях зберігання. Він є важливою складовою локальної політики безпеки комп'ютерної системи та дозволяє забезпечити захист від несанкціонованого доступу до конфіденційної інформації.

1.1.10 **Windows Update**

Windows Update - це вбудований сервіс оновлення операційної системи Windows, який надає користувачам можливість отримувати оновлення програмного забезпечення від Microsoft. Ось деякі ключові аспекти та функції Windows Update:

- Оновлення безпеки: Windows Update забезпечує постачання оновлень безпеки, які включають у себе виправлення вразливостей та патчі для захисту комп'ютера від шкідливого програмного забезпечення та інших загроз. Ці оновлення важливі для забезпечення безпеки комп'ютера та попередження можливих атак.

- Оновлення функціональності: Крім безпеки, Windows Update також надає оновлення функціональності операційної системи. Це можуть бути нові функції, покращення або виправлення проблем, які допомагають збільшити продуктивність та функціональні можливості вашої системи.
- Автоматичні оновлення: За замовчуванням, Windows Update налаштований на автоматичне отримання та встановлення оновлень. Це гарантує, що ваша система завжди отримує останні оновлення безпеки та функціональності. Автоматичні оновлення важливі для забезпечення безпеки та стабільності вашої комп'ютерної системи.
- Налаштування оновлень: Windows Update надає різні налаштування, які дозволяють вам контролювати процес оновлень. Ви можете вибрати, коли і як отримувати оновлення, включаючи розклад оновлень, виключення конкретних оновлень або використання підприємницьких налаштувань для управління оновленнями на корпоративному рівні.
- Додаткові компоненти: Крім самого Windows Update, Microsoft надає додаткові компоненти, такі як Microsoft Update і Windows Server Update Services (WSUS). Microsoft Update дозволяє отримувати оновлення не тільки для операційної системи Windows, але й для інших продуктів Microsoft, таких як Microsoft Office. WSUS надає можливість керування оновленнями на мережевому рівні в організаціях.

Windows Update є важливою складовою локальної політики безпеки комп'ютерної системи, оскільки вона забезпечує постачання оновлень безпеки та функціональності. Цей сервіс важливий для забезпечення безпеки, стабільності та оптимальної роботи вашої системи.

1.1.11 **Підписи драйверів Windows**

Підписи драйверів Windows - це механізм безпеки операційної системи Windows, який вимагає, щоб драйвери, які встановлюються на комп'ютер, були підписані цифровим сертифікатом. Ось деякі ключові аспекти та функції підписів драйверів Windows:

- Підтвердження автентичності: Підпис драйвера підтверджує, що драйвер був випущений відповідним виробником і не був змінений сторонніми особами. Це дозволяє впевнитись у тому, що драйвер походить від надійного джерела і не містить шкідливого або небезпечного коду.
- Цифровий сертифікат: Для підпису драйвера виробник повинен мати цифровий сертифікат, виданий авторитетним центром сертифікації (Certificate Authority).

  Цей сертифікат використовується для створення підпису, який забезпечує автентичність драйвера. Операційна система Windows перевіряє цифровий підпис, щоб переконатись, що драйвер є довіреним.
- Захист від шкідливого коду: Вимога до підпису драйверів допомагає запобігти використанню шкідливих або недовірених драйверів, які можуть потенційно пошкодити комп'ютер або вразити його безпеку. Це засіб захисту від встановлення драйверів з невідомого або ненадійного джерела.
- Політики підпису: Windows має різні політики підпису драйверів, які визначають, які типи підписів допускаються. Наприклад, в деяких версіях Windows вимагається обов'язковий цифровий підпис для всіх драйверів, тоді як інші версії можуть дозволяти встановлення непідписаних драйверів або попереджати про їхню недовіру.
- Виключення та ручні налаштування: В деяких випадках можна налаштувати операційну систему Windows для виключення підпису драйвера, якщо ви впевнені у його джерелі та безпеці. Проте це пов'язано

з певним ризиком і зазвичай не рекомендується для забезпечення безпеки системи.

Вони допомагають убезпечити систему від небажаного або шкідливого драйверного програмного забезпечення, забезпечують автентичність драйверів та зменшують ризик вразливостей.

1.1.12 **SMARTSCREEN**

SmartScreen є вбудованим сервісом безпеки, доступним в операційній системі Windows, який допомагає захищати користувачів від потенційно шкідливих інтернет-загроз, таких як шкідливі програми, фішингові атаки та шкідливі веб-сайти. На Рис. 2.6 можна побачити як спрацює SmartScreen захищаючи комп'ютер

Ось кілька ключових аспектів та функцій SmartScreen:

- Фільтрація шкідливих завантажень: SmartScreen аналізує файли, які ви намагаєтеся завантажити з Інтернету, і перевіряє їх на наявність відомих шкідливих програм. Якщо файл вважається небезпечним, SmartScreen видає попередження та може блокувати завантаження, щоб запобігти можливим загрозам для вашої системи.
- Захист від фішингу: SmartScreen виявляє фішингові веб-сайти, які намагаються використовувати соціальний інжиніринг для отримання вашої особистої інформації, такої як паролі або фінансові дані. Він може блокувати доступ до таких сайтів або відображати попередження для попередження вас про потенційну загрозу.
- Управління застосунками: SmartScreen може контролювати встановлення та виконання додатків, які не мають підпису від Microsoft або відомих видавців. Це допомагає запобігти запуску небезпечних або недовірених програм на вашій системі.

- Посилення безпеки веб-браузера: SmartScreen також використовується веб-браузерами Microsoft Edge та Internet Explorer для захисту від шкідливих веб-сайтів і завантажень. Він може блокувати веб-сторінки з відомим шкідливим змістом та попереджати про потенційні загрози.
- Налаштування SmartScreen: Користувачі мають можливість настроювати рівень захисту SmartScreen у своїй системі. Ви можете вибрати, як сервіс повинен реагувати на потенційно небезпечні файли та веб-сайти, або навіть вимкнути його повністю, хоча це не рекомендується з точки зору безпеки.

SmartScreen є важливою складовою безпеки в операційній системі Windows. Він допомагає захищати користувачів від шкідливих програм, фішингових атак та шкідливих веб-сайтів.

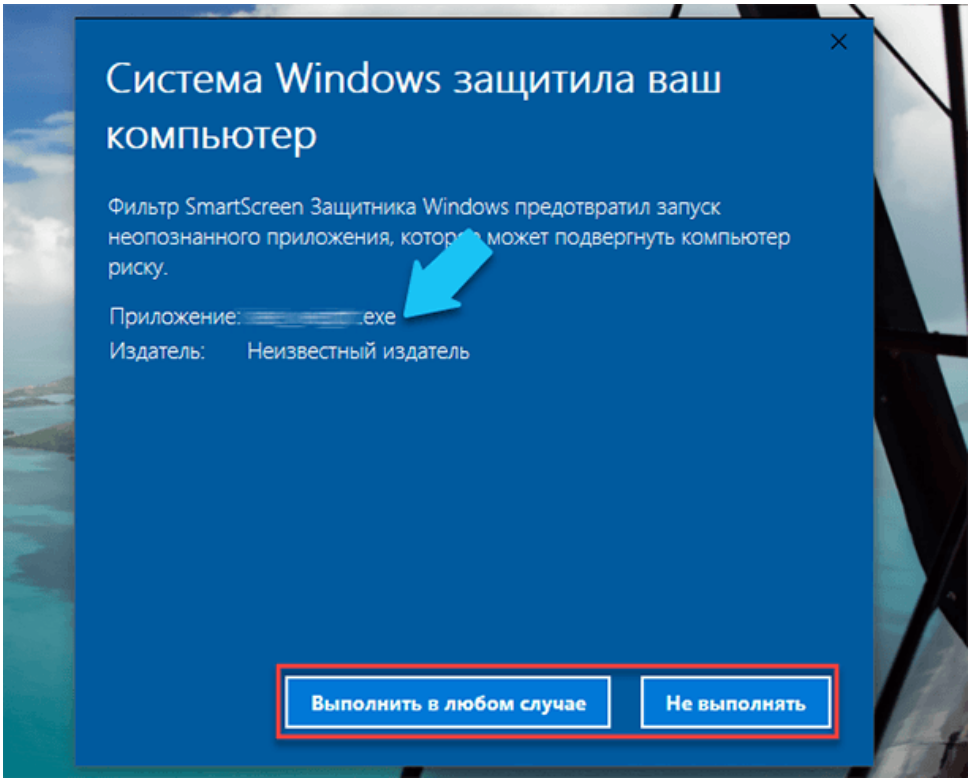


Рисунок 1.4- Попередження від SmartScreen про захист комп’ютера.

1.2 Файлова система NTFS

Абревіатура NTFS (New Technology File System) означає нова технологія файлової системи. NTFS є найбільш надійною системою спеціально розробленої для Windows NT і вдосконаленої в пізніших версіях Windows. Вона має характеристики захищеності, підтримуючи контроль доступу до даних і привілеї власника, що відіграють важливу роль у забезпеченні цілісності конфіденційних даних. Папки та файли NTFS можуть мати призначені їм права доступу незалежно від того, є вони спільними чи ні. Якщо файл буде скопійовано з розділу або тома NTFS у розділ або на тому FAT, всі права доступу та інші унікальні атрибути, властиві NTFS, будуть втрачені.

NTFS використовує 64-розрядні індекси кластерів, але Windows XP обмежує розміри томів NTFS до значень, при яких можлива адресація 32-розрядними кластерами, тобто до 128 Тб (з використанням кластерів по 64 Кб).

Одна з найважливіших властивостей NTFS - самовідновлення. При несподіваному збої системи інформація про структуру папок і файлів на томі FAT може бути втрачена. NTFS протоколює всі зміни, що дозволяє уникнути руйнування даних про структуру тома (у деяких випадках дані файлів можуть бути втрачені).

Здатність самовідновлення та підтримка цілісності реалізується за рахунок використання протоколу виконуваних дій та низки інших механізмів.

NTFS розглядає кожну операцію, що модифікує системні файли на NTFS-томах, як транзакцію (транзакція – сукупність операцій над даними, яка, з погляду обробки даних, або виконується повністю, або зовсім не виконується) і зберігає інформацію про таку транзакцію в протоколі. Почата транзакція може бути або повністю завершена (commit), або відкочується (rollback). В останньому випадку NTFS тому повертається в стан, що передує

початку транзакції. Для того, щоб керувати транзакціями, NTFS записує всі операції, що входять до транзакції, у файл протоколу, перед тим як здійснити запис на диск. Після того як транзакція завершена, всі операції виконуються. Таким чином, під керуванням NTFS не може бути незавершених операцій. У разі дискових збоїв незавершені операції скасовуються.

Під керуванням NTFS також виконуються операції, що дозволяють визначати дефектні кластери та відводити нові кластери для файлових операцій. Цей механізм називається cluster remapping. NTFS, в порівнянні з FAT, підтримує низку додаткових можливостей, основні з них:

- захист файлів та каталогів;
- стиснення файлів;
- Підтримка багатопоточних файлів;
- відстеження зв'язків;
- дискові квоти;
- шифрування;
- точки повторної обробки;
- точки з'єднання;
- тіньові копії.

Захист файлів та папок. Структурою NTFS передбачено зберігання для кожного файлу та кожної папки спеціального блоку безпеки, який містить таку інформацію:

- ідентифікатор (ім'я) користувача, який створив файл;
- список контролю доступу, в якому перераховані дозволи доступу до файлу або папки для користувачів та груп;
- системний список контролю доступу, в якому перераховано, які дії (наприклад, читання, запис тощо) для яких користувачів та груп необхідно фіксувати в журналі аудиту.

Це дозволяє операційній системі: забезпечувати розмежування доступу до файлів і папок і фіксувати дії, що виконуються користувачами над об'єктами. Оскільки на томах FAT подібна інформація не зберігається, то захист файлів і папок на них не здійснюється.

Стиснення файлів та каталогів. NTFS забезпечує динамічний стиск файлів та каталогів. Стиснення є атрибутом файлу або каталогу, який можна зняти або встановити. Стиснення можливе лише на розділах, розмір блоку яких не перевищує 4096 байт. Якщо каталог має атрибут стислий (compressed), всі файли, що копіюються в нього, теж отримають цей атрибут. Продуктивність комп'ютера при використанні стислих файлів зростає до 50% залежно від типу даних, що зберігаються.

Такий результат досягається за рахунок підвищення завантаження процесора в 3-5 разів. Однак на великих (більше 4 Гб) розділах і на стійких до відмови томов продуктивність помітно знижується. Тому рекомендується використовувати функцію стиснення на невеликих томах у комп'ютерах зі швидкими процесорами чи багатопроцесорних системах.

Дозволи NTFS дозволяють явно вказати, які користувачі та групи мають доступ до файлів і папок і які операції з вмістом цих файлів і папок їм дозволено виконувати. Застосовувати дозволи NTFS можна лише до ресурсів дискових томів, відформатованих з використанням файлової системи NTFS. Дозволи для папок встановлюються для керування доступом користувачів до вкладених папок і файлів, які містяться в цих папках.

1.2.1 Планування та встановлення дозволів NTFS.

Для початку створюю облікові записи користувачів групи "Адміністратори", використовуючи наступну інформацію:
Василій Обмежений обліковий запис

Віталій Обмежений обліковий запис

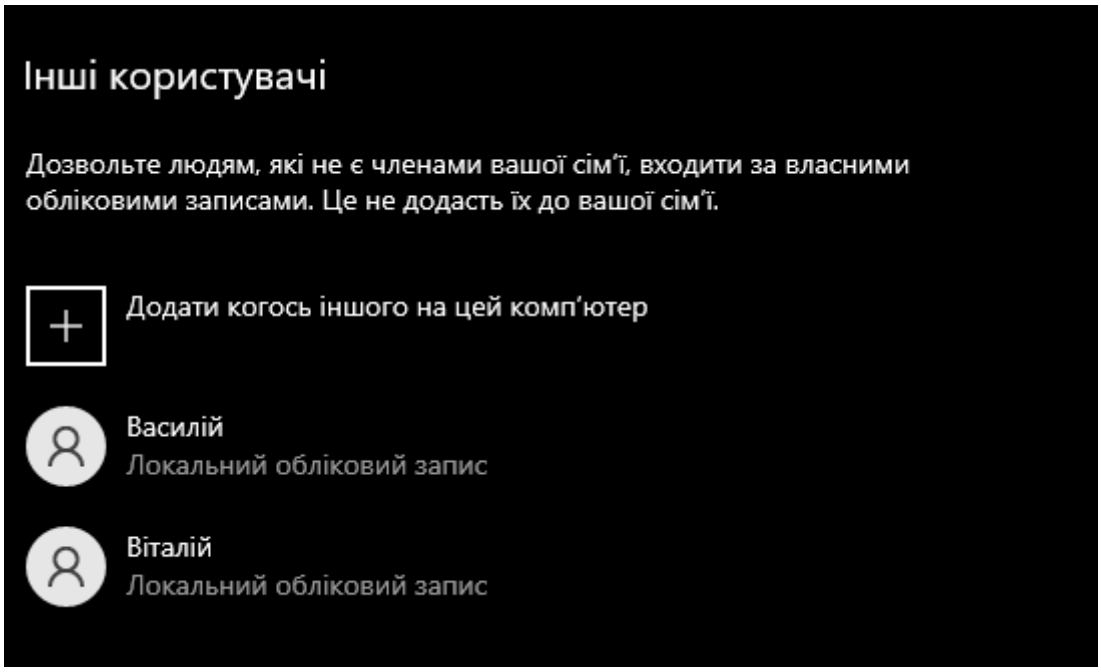


Рисунок 1.5 Інтерфейс для додавання Користувачів

1.Наступним кроком створюю папки

D:\Public;

D:\Public\Library.

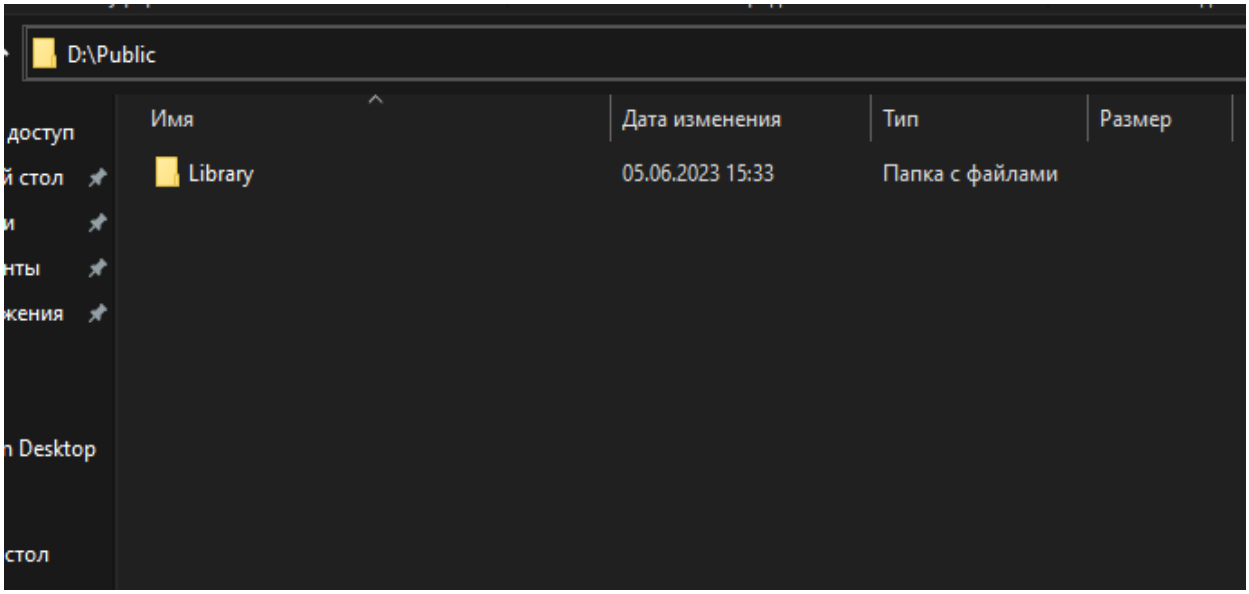


Рисунок 1.6 Папка Public

2. Переходжу в "Мій комп'ютер" і обираю "Провідник".

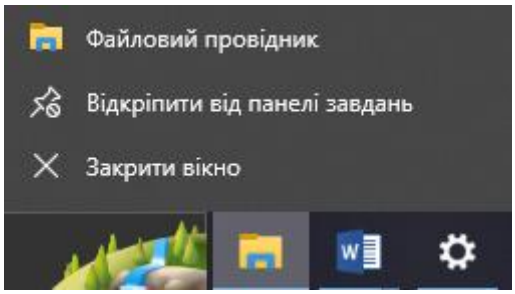


Рисунок 1.7 Провідник

3. Відкриваю локальний диск D:, заходжу до папки “Public” і обираю "Властивості"; після чого з'явиться діалогове вікно "Властивості спільної папки" з вибраною вкладкою "Загальні".

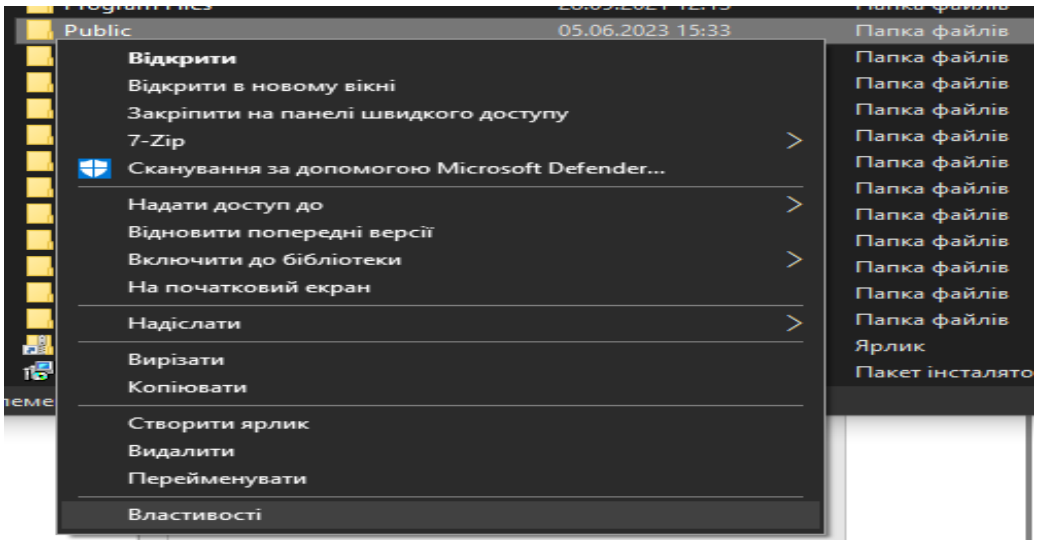


Рисунок 1.8 Контексне меню для папки Public

4. Переходжу на вкладку "Безпека", щоб переглянути дозволи, встановлені для спільної теки.

Якщо користувач або група має спеціальні дозволи, обираю користувача або групу і Натискаю кнопку "Додатково", щоб відобразити список спеціальних дозволів.

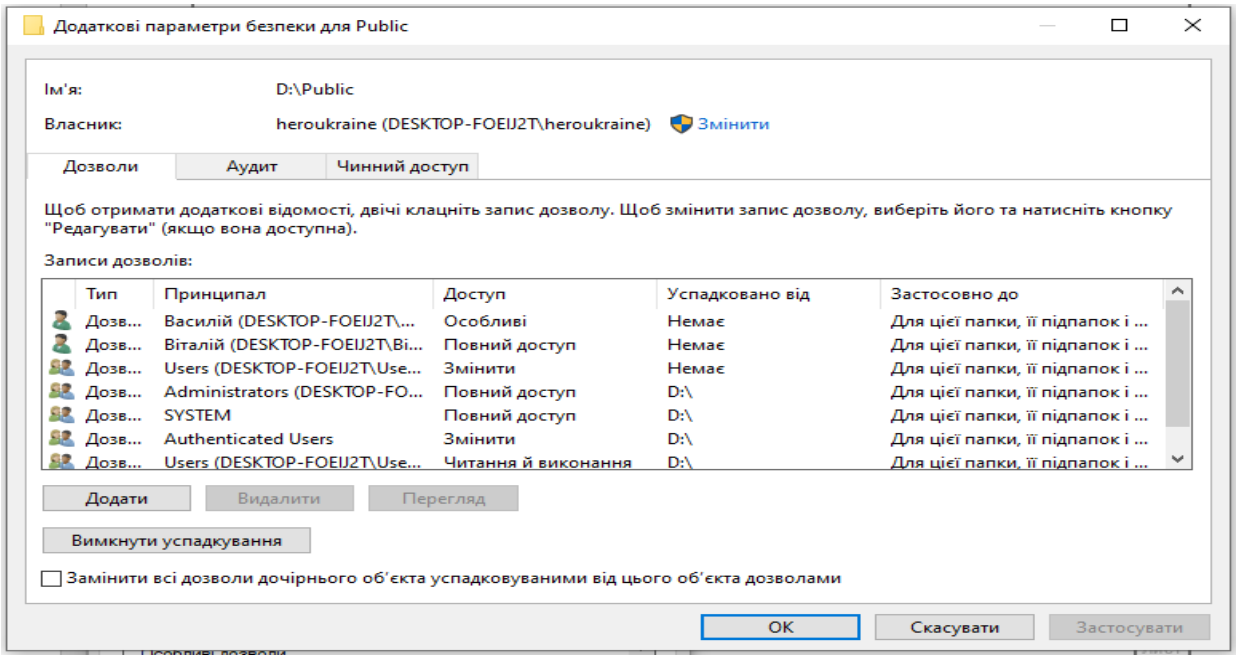


Рисунок 1.9 Вікно Додаткових параметрів безпеки для папки Public

5. Натискаю ОК, щоб закрити діалогове вікно Властивості спільної теки.

6. Закриваю вікно Провідника і виходжу з системи.

Перевірка дозволів, встановлених для папки Public

1. Входжу до системи за допомогою облікового запису Василій, а потім запускаю Провідник.

2. Переходжу до папки Public.

3. У папці Public створюю текстовий документ, називаю його Test 1 і вводжу наступний текст: Перевірка дозволів, встановлених для папки.

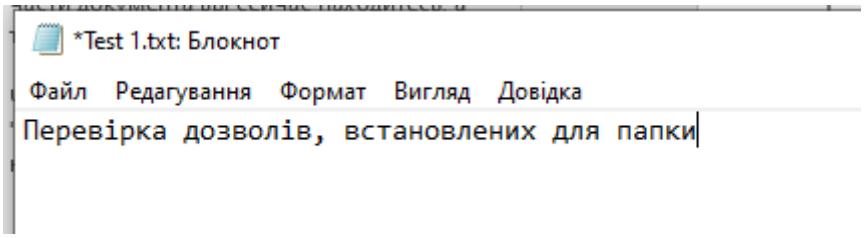


Рисунок 1.10 Відкритий текстовий файл Test 1

4. Пробую виконати такі операції зі створеним файлом:

- Відкриваю файл;

• Змінюю файл;

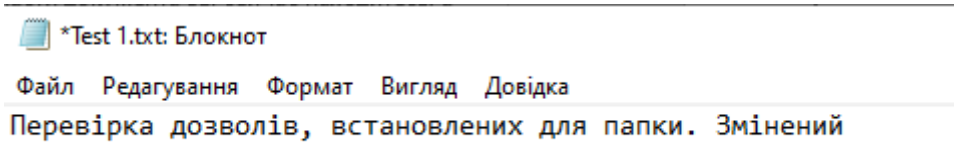


Рисунок 1.11 Зміненний текстовий файл Test 1

• Видаляю файл.

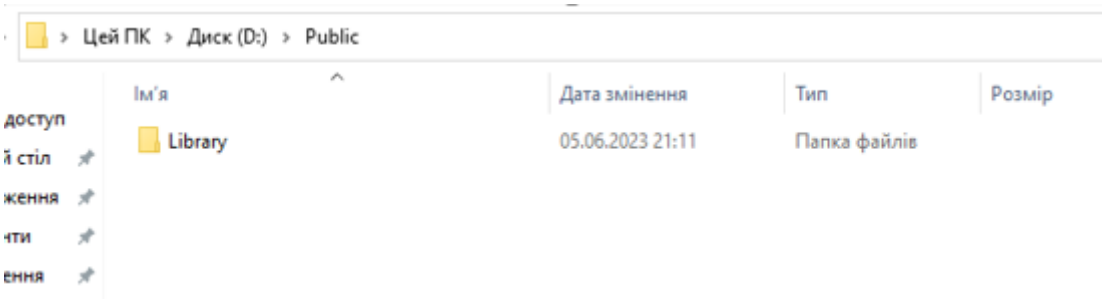


Рисунок 1.12 Папка Public, після видалення текстового файла Test 1

5. У папці Public знову створюю текстовий документ Test 1.

6. Виходжу з системи

7. Входжу до системи за допомогою облікового запису Віталій.

8. Виконую такі операції з текстовим документом Test 1:

• Відкриваю файл;

• Змінюю файл;

• Видаляю файл.

Я проробив ці дії, щоб можна було побачити, що кожен обліковий запис має права, щоб створювати , видаляти та змінять файли у папці Public

Встановлення дозволів NTFS

Далі я встановлю дозволи NTFS для папки Public відповідно до наступної політики:

• усі користувачі повинні мати можливість читати документи та файли у папці Public;

• усі користувачі повинні мати можливість створювати документи у папці Public;

• усі користувачі повинні мати можливість змінювати зміст, властивості та дозволи для створюваних ними документів у папці Public;

• Користувач Віталій несе відповідальність за тримання папки Public і повинен мати можливість змінювати та видаляти всі файли в папці Public.

В даний час мій реєстраційний запис – Віталій.

Встановлення дозволів NTFS для папки

1. Входжу у систему, використовуючи обліковий запис члена групи Адміністратори (Administrators). Відкриваю Провідник (Windows Explorer).

2. Відкриваю папку Public.

3. Заходжу до Властивості (Properties) папки Public.

4. Переходжу на вкладку Безпека діалогового вікна властивостей папки.

5. На вкладці Безпека Натискаю кнопку Додати. Відкриється діалогове вікно Вибір: користувачі або групи.

6. У текстовому полі Введіть імена об'єктів, що вибираються (Enter The Object Names To Select) ввожу Віталій, потім натискаю Перевірити імена. У текстовому полі Введіть імена об'єктів, що вибираються (Enter The Object Names To Select) повинен з'явитися напис DESKTOP-FOEIJ2T \ Віталій. Це свідчить, що Windows 10виявила користувача Віталій на комп'ютері DESKTOP-FOEIJ2T і що це дійсний обліковий запис користувача.

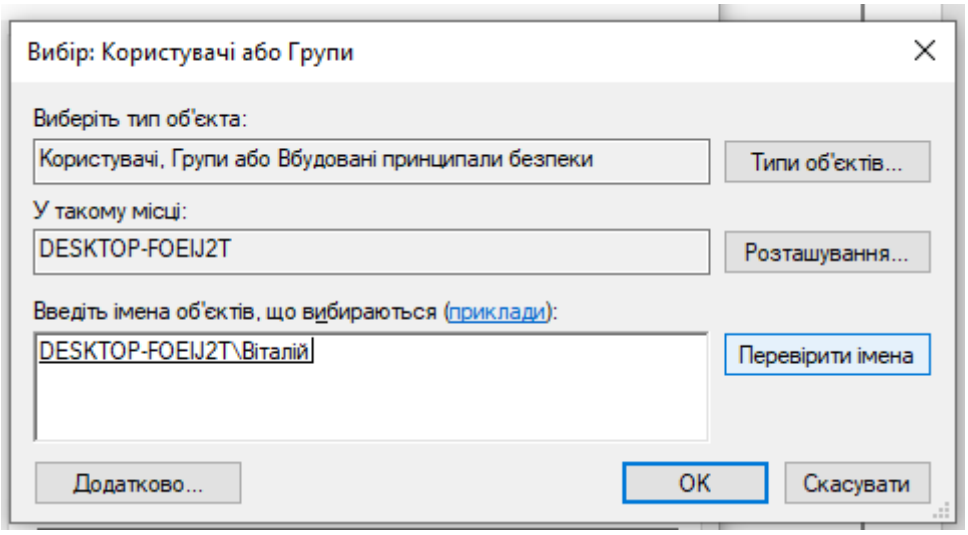


Рисунок 1.13 Вікно для вибора Користувачів або Групи

7. Натискаю кнопку ОК, щоб закрити діалогове вікно Вибір: Користувачі або групи. Тепер користувач Віталій включений до списку Групи або користувачі (Group Or User Name) діалогового вікна властивостей папки Public.
8. Натискаю кнопку Додатково (Advanced). Відкриється діалогове вікно Додаткові параметри безпеки для Public (Advanced Security Settings For Public), і можна побачити, що користувач Віталій (DESKTOP-FOEIJ2T \ Віталій) включений до списку Елементи дозволів (Permissions Entries).
9. Дивлюся, щоб рядок Віталій виділено, і натискаюя кнопку Змінити (Edit). Відкриється діалогове вікно Запис дозволу для Public (Permission Entry For Public), і можна побачити обліковий запис користувача Віталій (DESKTOP-FOEIJ2T\Віталій) у текстовому полі Ім'я (Name).
10. У колонці Дозволити (Allow) натискаю на прапорець Повний доступ (Full Con-trol). Тепер у стовпчику Дозволити (Allow) встановлені всі прапорці.
11.Натискаю ОК, щоб закрити діалогове вікно Елемент дозволу для Public.

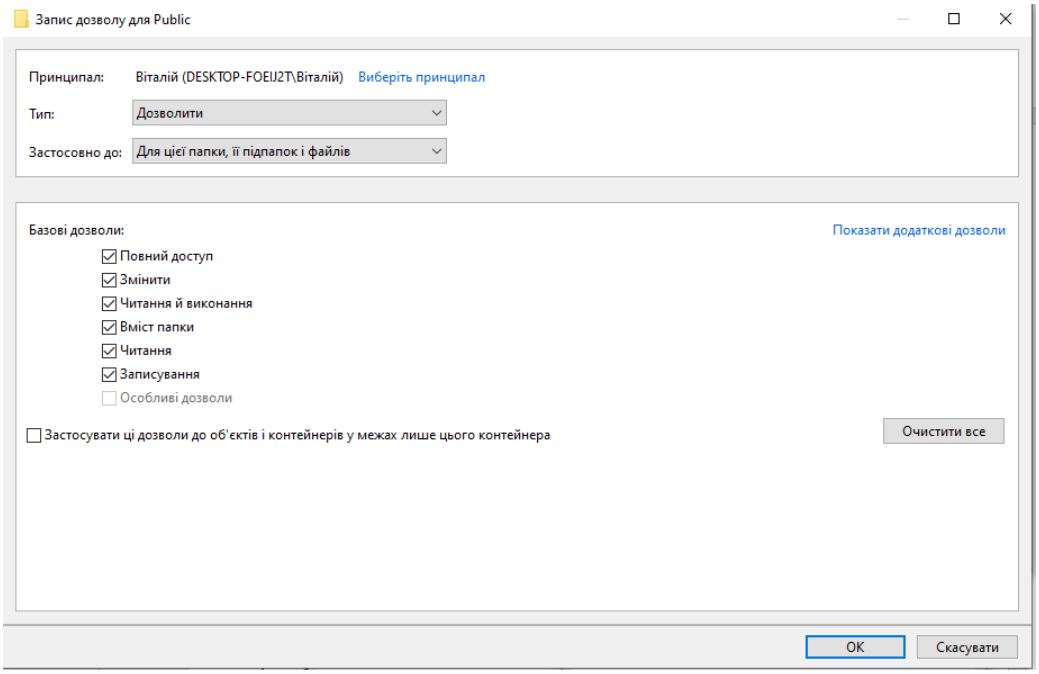


Рисунок 1.14 Вікно запису дозволів для папки Public

12. Натискаю кнопку ОК, щоб закрити діалогове вікно Додаткові параметри безпеки для Public (Advanced Security Settings For Public).

13. Натискаю кнопку ОК, щоб закрити діалогове вікно властивостей папки Public.

14. Закриваю Провідник (Explorer) та завершаю сеанс роботи.

Перевірка дозволів NTFS для папки

1. Заходжу у систему, використовуючи обліковий запис Віталій

2. Запускаю Провідник (Explorer).

3. Відкриваю диск D:, а потім відкриваю папку Public.

4. Спробую зробити такі дії з текстовим документом Test 1:

- Відкрити файл;
- Змінити файл;
- Видалити файл.

Оскільки до цього , я виставив у властивостях повний доступ користовачу Віталій , то я зміг виконати усі дії з файлом

Перевірка дозволів NTFS

Створюю файл у підпапці та перевіряю, як дозволи NTFS наслідуються в ієрархії папок.

Перевірка дозволів для папки Library

1. Входжу до системи за допомогою облікового запису Василій і запускаю Провідник (Windows Explorer).

2. У Провіднику (Windows Explorer) відкриваю папку Public\Library.

3. Створюю текстовий документ Test 1 у папці Library.

4. Завершую сеанс Windows 10.

Перевірка дозволів для папки Library з використанням підключення з обліковим записом Віталій

1. Заходжу в системи за допомогою облікового запису Віталій. потім запускаю Провідник (Windows Explorer).

2. Відкриваю папку Public/Library.

3. Пробую зробити такі дії з текстовим документом Test 1:

• відкрити файл;

• змінити файл;

• видалити файл.

4. Завершую роботу з Windows 10.

Оскільки папка Library знаходиться всередині папки Public, то дозволи успадковуються до неї, тому усі дії я зміг зробити, бо мав такий самий доступ.

1.2.2 Зміна дозволів NTFS.Зміна власника файлу

Для зміни власника файлу необхідно визначити дозволи для файлу, встановити дозвіл Зміна власника (Take Ownership) для облікового запису користувача і стати власником файлу.

Визначення дозволів для файлу

1. Входжу у систему, використовуючи обліковий запис члена групи Адміністратори.

2. У папці Public створюю текстовий документ та називаю його OWNER.

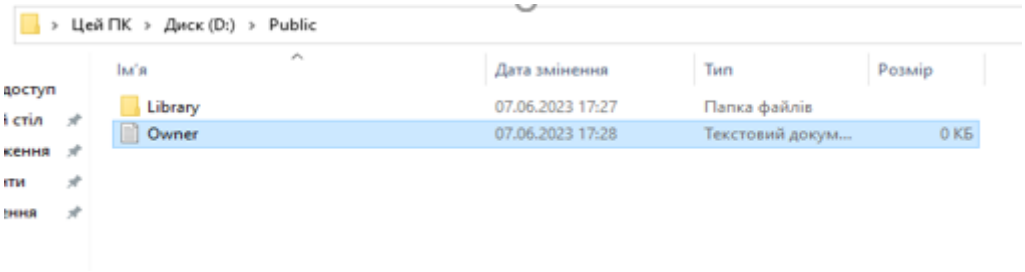


Рисунок 1.15 Папка Public з файлом OWNER

3. Заходжу Властивості (Properties) документа OWNER. У Microsoft Windows 10 відкриється діалогове вікно Властивості: Owner (Owner Properties) з активною вкладкою Загальні (General).

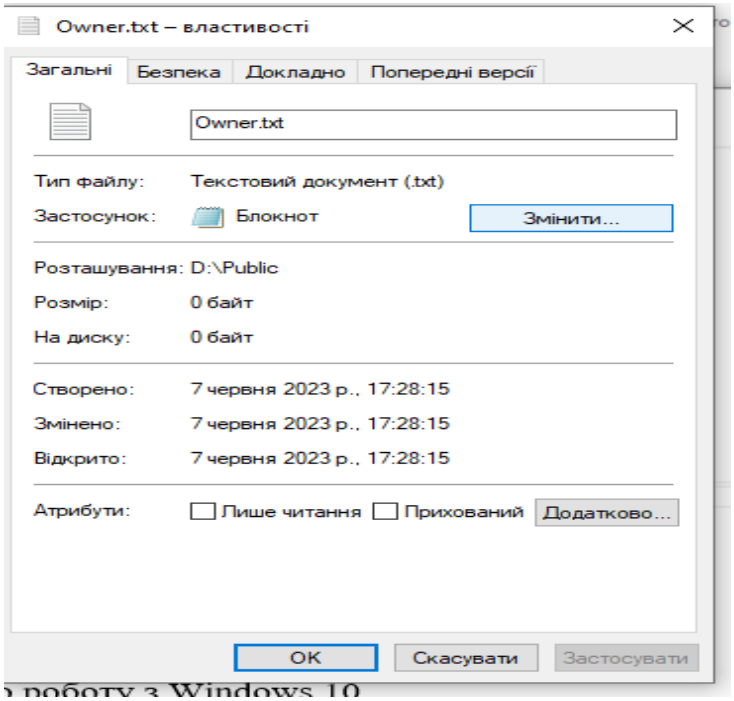


Рисунок 1.16 Вікно з властивостями файла OWNER

4. Переходжу на вкладку Безпека (Security) для перегляду рішень, встановлених для файлу OWNER.

5. Натискаю кнопку Додатково (Advanced). Відкриється діалогове вікно Додаткові параметри безпеки для Owner (Advanced Security Settings For Owner) з активною вкладкою Дозволи

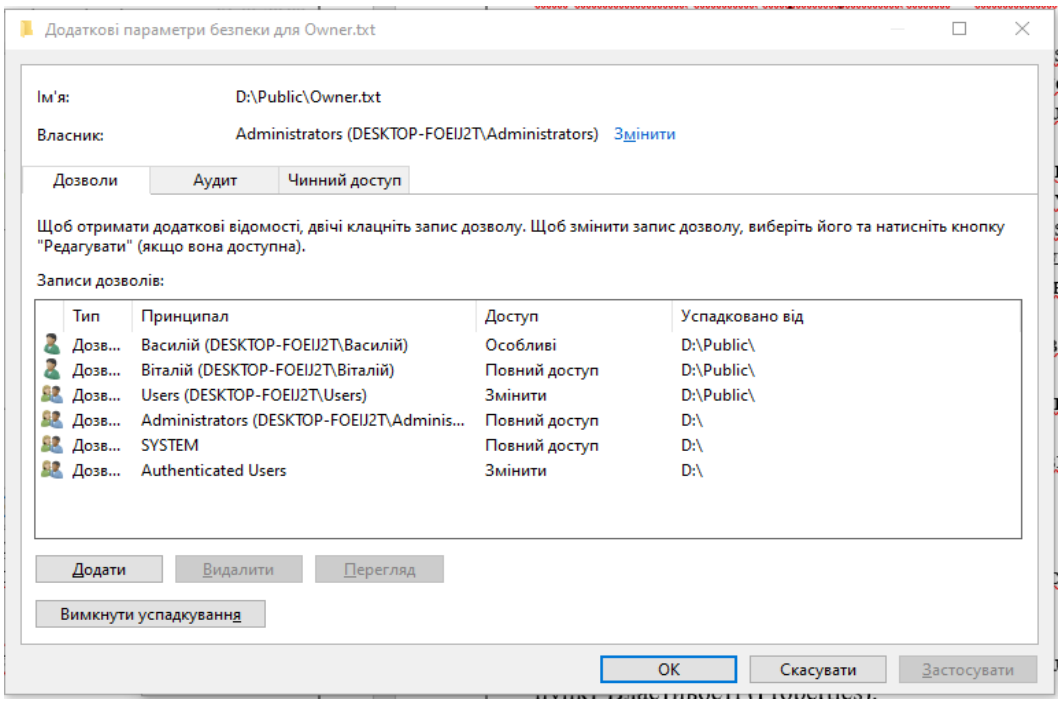


Рисунок 1.17 Вікно Додаткові параметри безпеки для Owner

6. Тут можна побачити , що власником є Administrators

Встановлення дозволу, який дозволяє користувачеві змінити власника

1. У діалоговому вікні Додаткові параметри безпеки для Owner (Advanced Security Settings For Owner) переходжу на вкладку Дозволи (Permissions).

2. Натискаю кнопку Додати (Add). Відкриється діалогове вікно Вибір: користувачі або групи (Select Users Or Groups).

3. Переконуюся, що в текстовому полі Розміщення (From This Location), яке розташоване вгорі діалогового вікна, вибрано ім'я комп'ютера (DESKTOP-FOEIJ2T).

4. У текстовому полі Введіть імена об'єктів, що вибираються (Enter The Object Names To Select) введіть Василій потім натискаю Перевірити імена (Check Names).

У списку Введіть імена об'єктів, що вибираються (Enter The Object Names To Select) повинен з'явитися запис DESKTOP-FOEIJ2T\ Василій. Це означає, що обліковий запис користувача Василій знайдено на комп'ютері з ім'ям DESKTOP-FOEIJ2T і є дійсним обліковим записом.

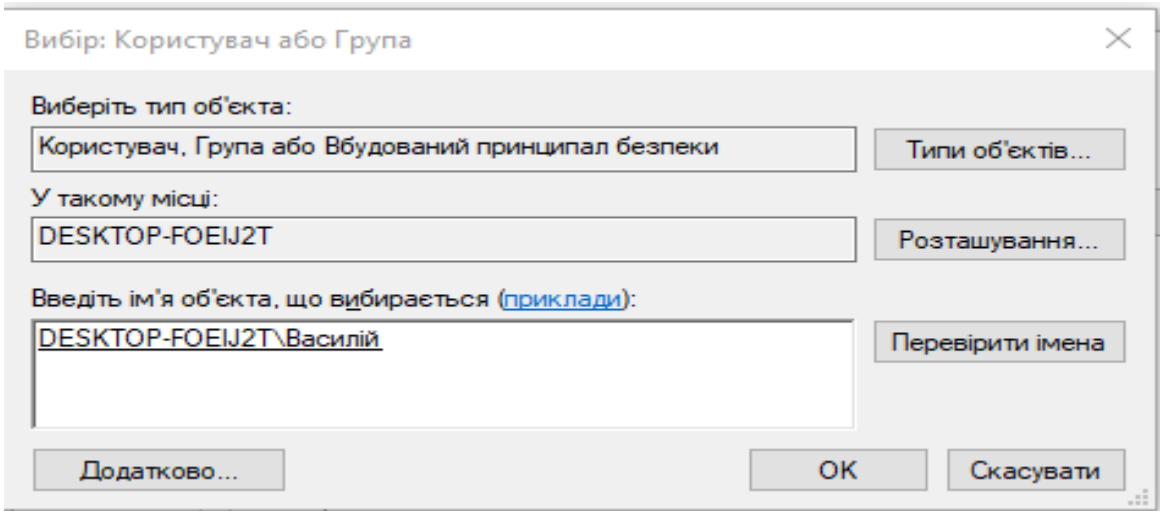


Рисунок 1.18 Вікно для вибора користувача

5. Натискаю кнопку ОК. У Windows 10 стане активним діалогове вікно Елемент дозволу для Owner (Permission Entry For Owner). Звертаю увагу, що всі елементи дозволів для користувача Василій не позначені.

6. У колонці Дозволи (Permissions) встановлюю прапорець Дозволити (Allow) для дозволу Змінити власника (Take Ownership).

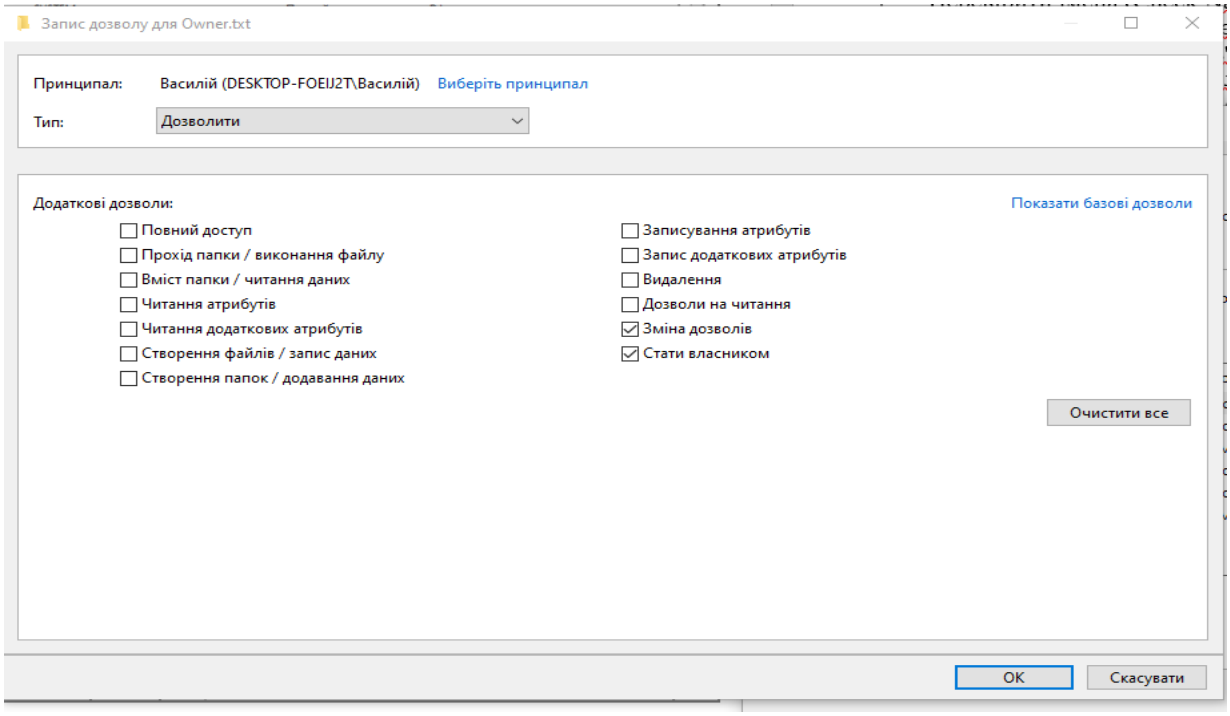


Рисунок 1.19 Змінення дозволів для користувача Василій

7. Натискаю кнопку ОК. У Windows 10 стане активним діалогове вікно Додаткові параметри безпеки для Owner (Advanced Security Settings For Owner) з відкритою вкладкою Дозволи (Permissions).

8. Натискаю ОК, щоб повернутися до діалогового вікна властивостей файлу OWNER.

9. Натискаю ОК, щоб зберегти зміни, і Закриваю діалогове вікно властивостей файлу OWNER.

10. Закриваю Провідник (Windows Explorer) і виходжу із системи.

Зміна власника файлу

1. Входжу в системі, використовуючи обліковий запис Василій і запускаю Провідник.

2. Входжу до папки Public.

3. Натискаю значок файлу OWNER і обираю пункт Властивості (Properties).

4. Переходжу на вкладку Безпека (Security) для перегляду рішень для файлу.

5. Натискаю кнопку Додатково (Advanced), щоб відкрити діалогове вікно Додаткові параметри безпеки для Owner (Advanced Se-curity Settings For Owner) і Переходжу на вкладку Власник (Owner).

6. У колонці Змінити власника на (Change Owner To) обираю Василій, а потім натискаю кнопку Застосувати (Apply).

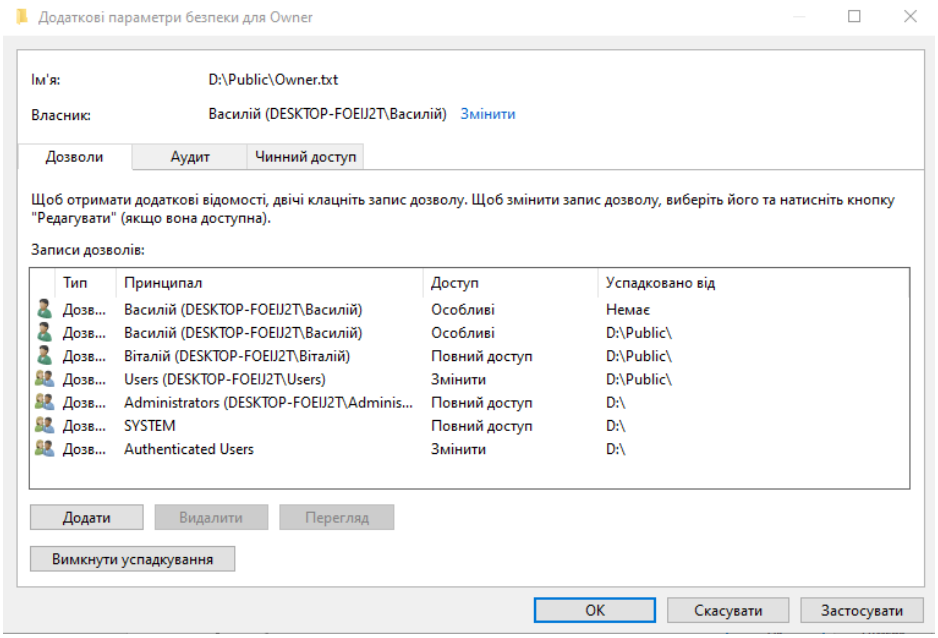


Рисунок 1.20 Вже зміненний власник файлу Owner

7. Натискаю кнопку ОК, щоб закрити діалогове вікно Додаткові параметри безпеки для Owner (Advanced Security Settings For Owner).

8. Натискаю кнопку ОК, щоб закрити діалогове вікно властивостей файлу OWNER.

Перевірка дозволів для файлу як власника

1. Поки я підключений як Василій, встановлюю роздільну здатність Повний доступ (Full Control) користувачеві Василій до текстового документа OWNER і ОК.

2. Настикаю Додатково (Advanced) і знімаю прапорець Спадкоємство від батьківського об'єкта, що застосовується до дочірніх об'єктів дозволу, додаючи їх до явно заданих у цьому вікні (Inherit From Parent).

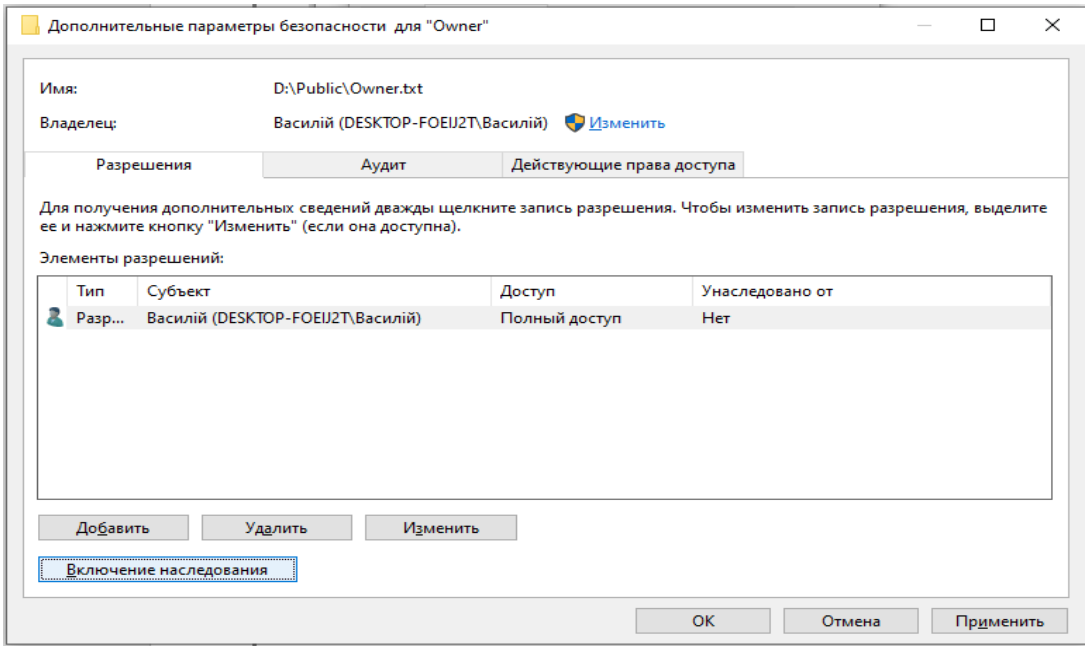


Рисунок 1.21 Прибирання Спадкоємство від батьківського об'єкта для користувача Василій

3. У діалоговому вікні Безпека (Security) натискаю кнопку Видалити (Remove).

4. Натискаю кнопку ОК, щоб закрити діалогове вікно Додаткові параметри безпеки для Owner (Advanced Security Settings For Owner).

5. Натискаю кнопку ОК, щоб закрити діалогове вікно властивостей файлу OWNER.

6. Видаляю текстовий документ OWNER.

1.2.3 **Копіювання та переміщення папок.**

Створення папки під час підключення до облікового запису користувача 1. Входжу в систему під обліковим записом Василій , у Провіднику (Windows Explorer), у кореневій папці диска D: створюю папку з ім'ям Temp1.

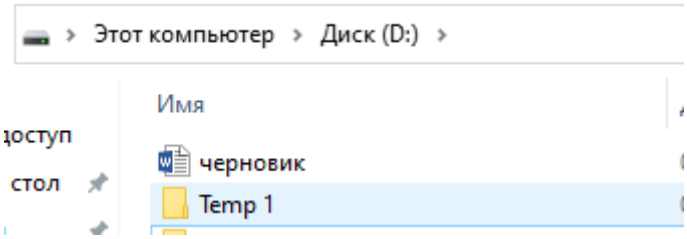


Рисунок 1.22 Створена папка Temp 1

2. Закриваю всі програми та закінчіть роботу з Windows 10.

Створення папки при підключенні з обліковим записом члена групи Адміністратори (Administrators)

1. Входжу у систему, використовуючи обліковий запис члена групи Адміністратори і запускаю Провідник (Windows Explorer).

2. У кореневій папці диска D: створюю папки Temp2 і Temp3.

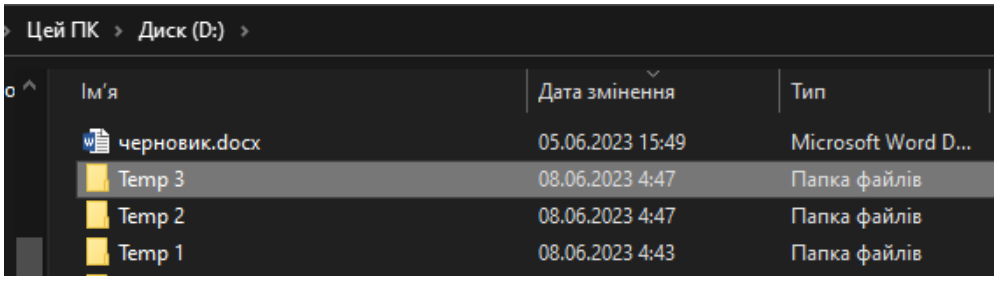


Рисунок 1.23 Створені папки Temp 2 і Temp 3

3. Встановлюю роздільну здатність для папок Temp2 і Temp3 (таблиця 1.). Знімаю прапорець Успадкувати від батьківського об'єкта дозволені дочірні об'єкти дозволу, додаючи їх до явно заданих у цьому вікні. У діалоговому вікні, що відкрилося, натискаю Видалити (Remove) для видалення всіх дозволів, крім зазначених явно.Параметри роздільної здатності для папок Терм2 і Терм3.

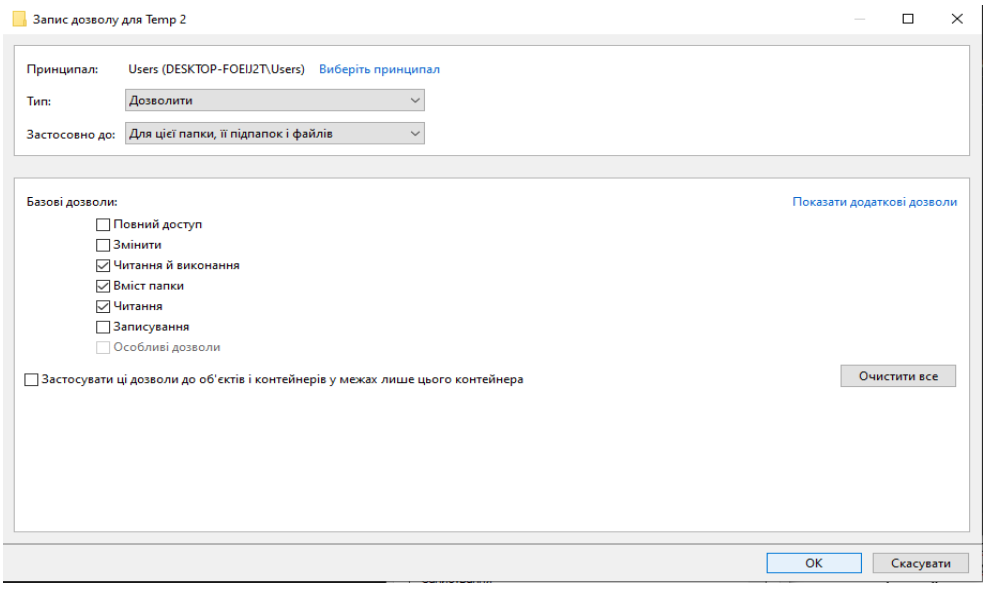


Рисунок 1.24 Параметри запису дозовлу для папки Temp 2

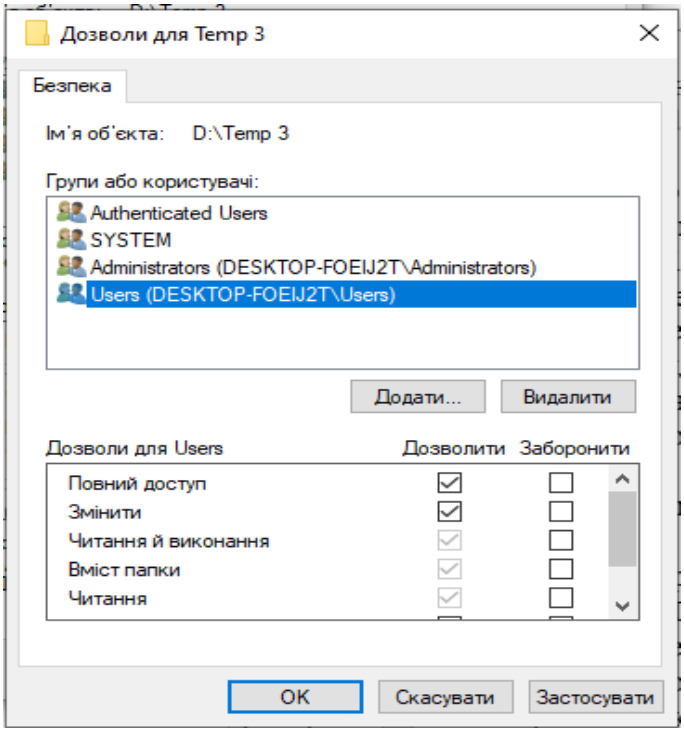


Рисунок 1.25 Параметри роздільної здатності для папки Терм3.

Таблиця 1.2 Потрібні дозволи для папок Temp 2 і Temp 3

Папка	Встановлюю такі дозволи
Temp2	Адміністратори (Administrators): Повний доступ (Full Control) Користувачі (Users): Читання та виконання (Read & Execute)
Temp3	Адміністратори (Administrators): Повний доступ (Full Control)) Користувачі (Users): Повний доступ (Full Control)

Копіювання папки в іншу папку на тому самому томі NTFS у Windows 10

1. Увійшовши в систему під обліковим записом члена групи Адміністратори (Administrators), у Провіднику (Windows Explorer), скопіюю папку D:\Temp2 в папку D:\Temp1. Оскільки була проведена операція копіювання, повинні існувати обидві папки: D:\Temp2 і D:\Templ\Temp2.

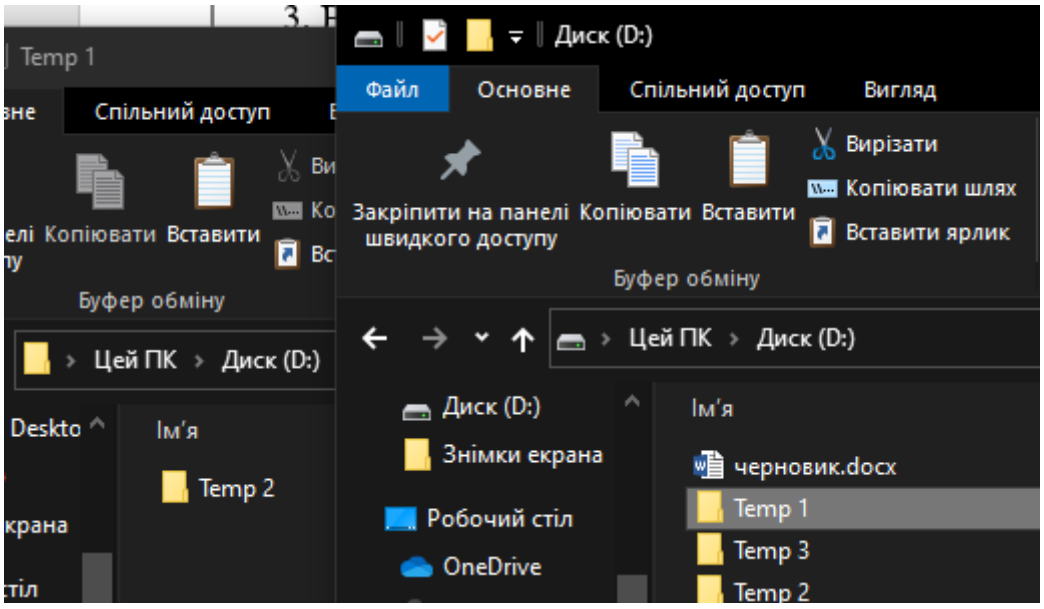


Рисунок 1.26 Копіювання папки Temp 2 до папки Temp 1

2. Виділяю D:\Templ\Temp2, потім порівнюю дозволи та права власника з папкою D:\Temp2 і можна побачити, що обидві папки мають однакові дозволи та права

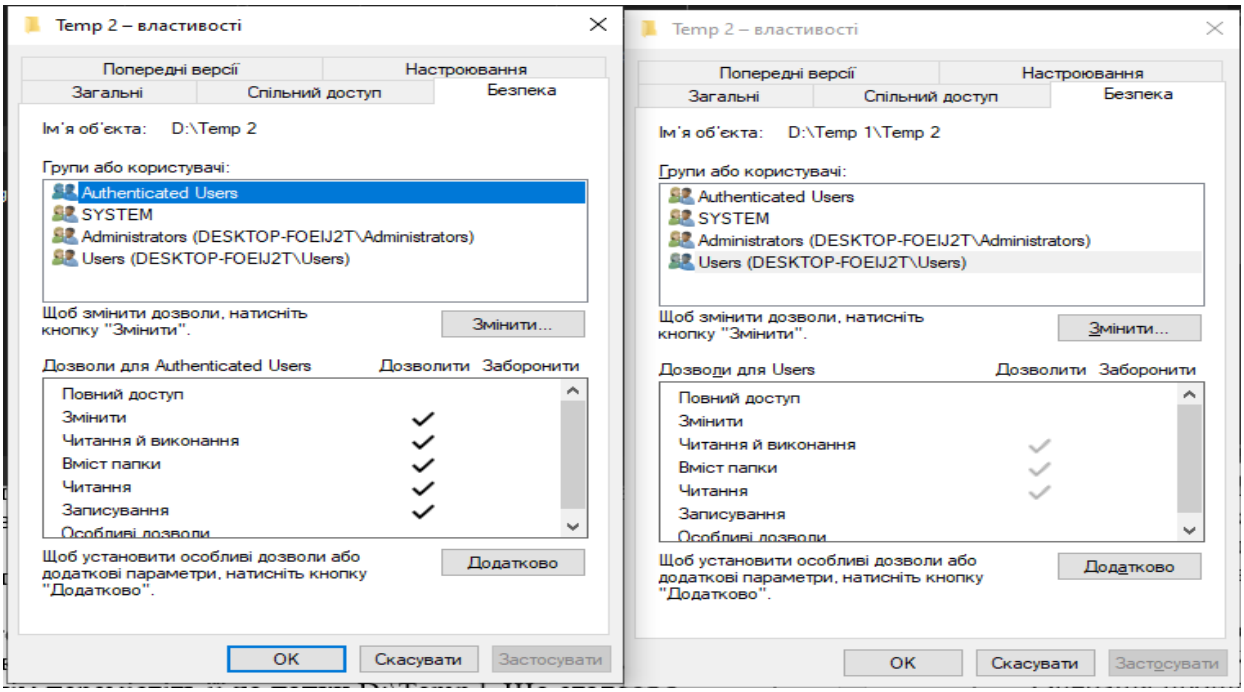


Рисунок 1.27 Зрівняння дозволів для папок у різних директоріях

Переміщення папки на тому самому томі

1. Увійду в систему як користувач Василій.

2. У Провіднику переходжу до піктограми папки D:\Temp 3. потім переміщаю її до папки D:\Temp l.

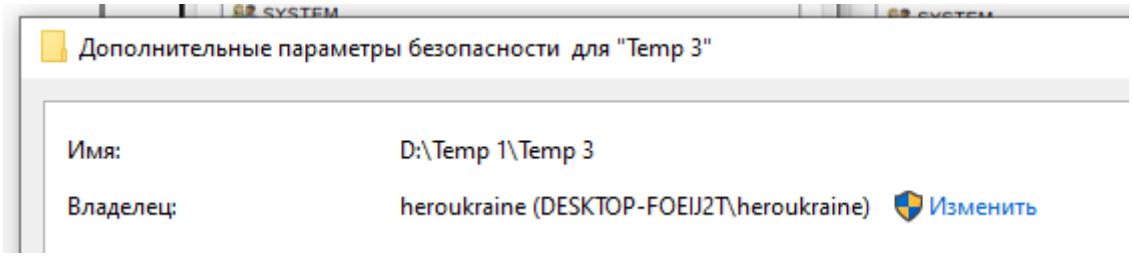


Рисунок 1.28 Власник папки Temp 3

3. Закриваю всі вікна та завершую сеанс роботи.

Видалення файлу, для якого встановлено заборону на всі дозволи

Створюю файл у папці Темр 3, до якої надано дозвіл Повний доступ (Full Control) групі Користувачі (Users), але заборонюю усі дозволи для нього.

Створення файлу та заборона доступу до нього

1. Входжу у систему, використовуючи обліковий запис члена групи Адміністратори (Administrators).

2. У папці D:\Temp l\Temp 3 створюю текстовий документ з ім'ям WITHOUTACCESS.

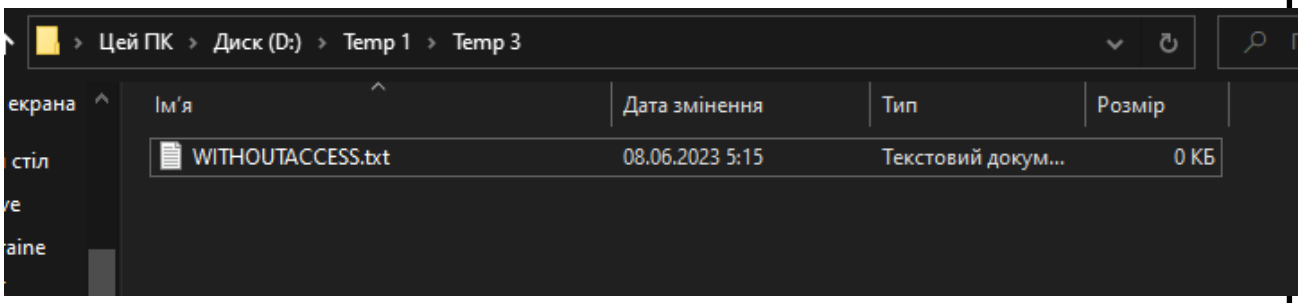


Рисунок 1.29 Файл WITHOUTACCESS у папці

3. Забороняю для групи Користувачі (Users) дозвіл Повний доступ (Full Control) для текстового документа WITHOUTACCESS.

У Windows 10 з'явиться діалогове вікно Безпека (Se-curity) з наступним повідомленням: «Ви заборонили доступ до WITHOUTACCESS.txt. Ніхто не зможе отримати доступ до WITHOUTACCESS.txt, і тільки власник зможе змінити дозволи. Продовжити виконання операції?»

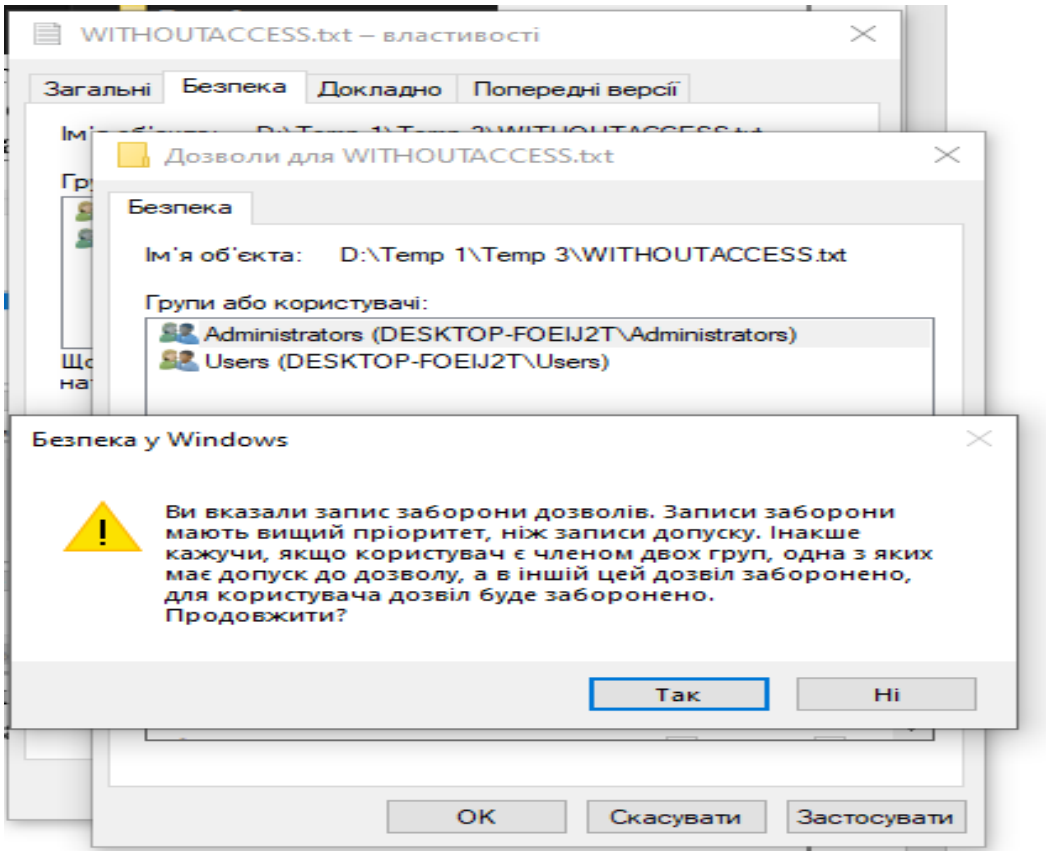


Рисунок 1.30 Попередження про заборону дозволу до файла WITHOUTACCESS усім користувачам

4. Натискаю Так (Yes), щоб зміни набули чинності і щоб закрити діалогове вікно Безпека (Security).

5. Натискаю кнопку ОК, щоб закрити діалогове вікно властивостей файлу WITHOUTACCESS.

Перегляд результату заборони дозволу Повний доступ до папки

1. У Провіднику (Windows Explorer) переходжу до документа WITHOUTACCESS у папці Temp3 для того, щоб відкрити його. Але нічого не виходить , бо я обмежив доступ для усіх користувачів.

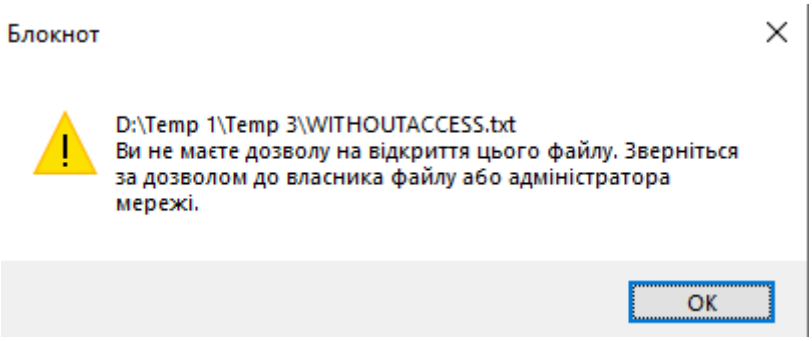


Рисунок 1.31 Повідомлення про недостатність прав для відкриття файлу WITHOUTACCESS

2. Натискаю Пуск (Start), потім — Виконати (Run). Windows 10 відкриється діалогове вікно Виконати (Run).

3. Введіть cmd в текстовому полі Відкрити (Open) і Натискаю кнопку ОК.

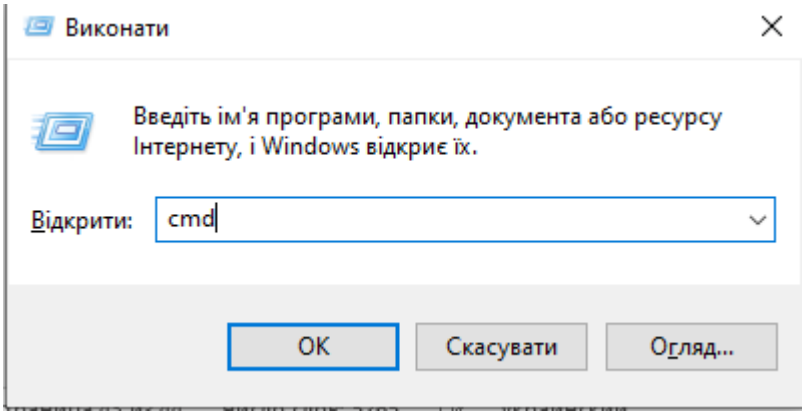


Рисунок 1.32 Відкриття командного рядка(консолі)

4. Переходжу до папки D:\Templ\Temp3.

Ввожу Del "D:\Temp 1\Temp 3\WITHOUTACCESS.TXT та натискаю ENTER.

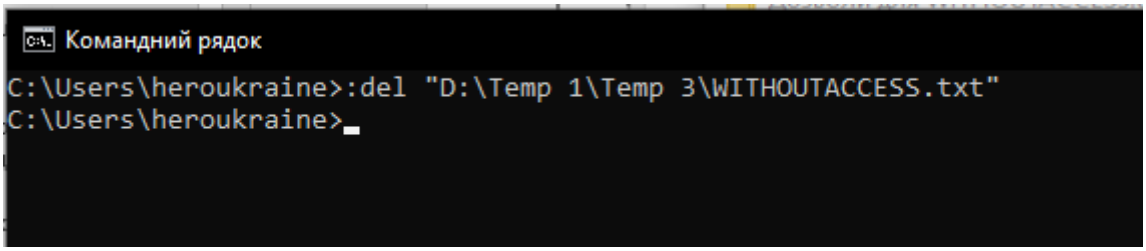


Рисунок 1.33 Інтерфейс командного рядка з виконаною командою для видалення файлу WITHOUTACCESS

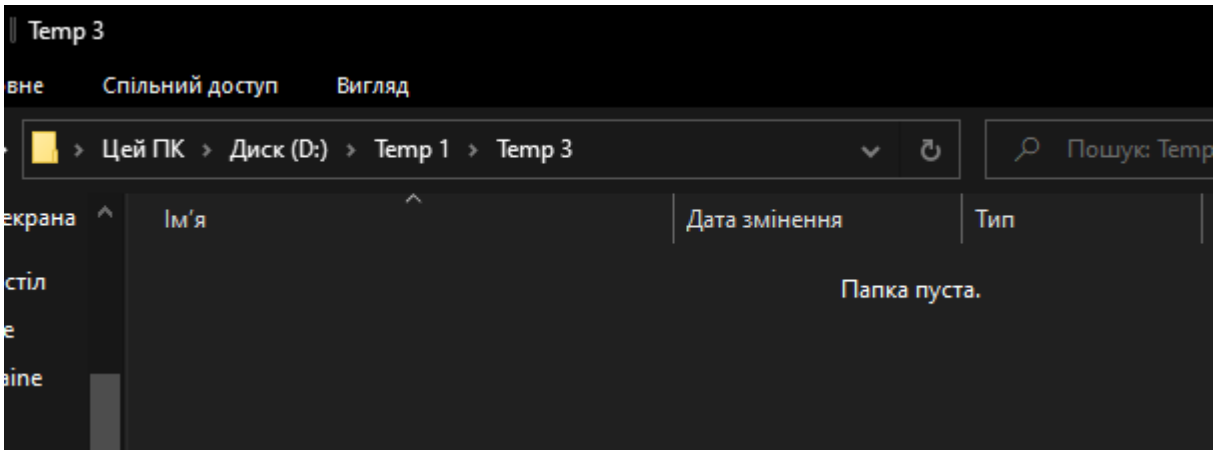
6. 

Рисунок 1.33 Пуста папка Temp 3 після видалення файлу WITHOUTACCESS

Мені вдалося видалити файл WITHOUTACCESS, тому що командний рядок має дозвіл Адміністратора. Але мені б не вдалося цього зробити ,якби я був під обліковим записом Василій або Віталій, бо доступ їм обмежен до цього файлу і при спробі видалити файл побачив вікно, де написано що я не маю доступу для цього. Приклад можно побачити на Рисунку

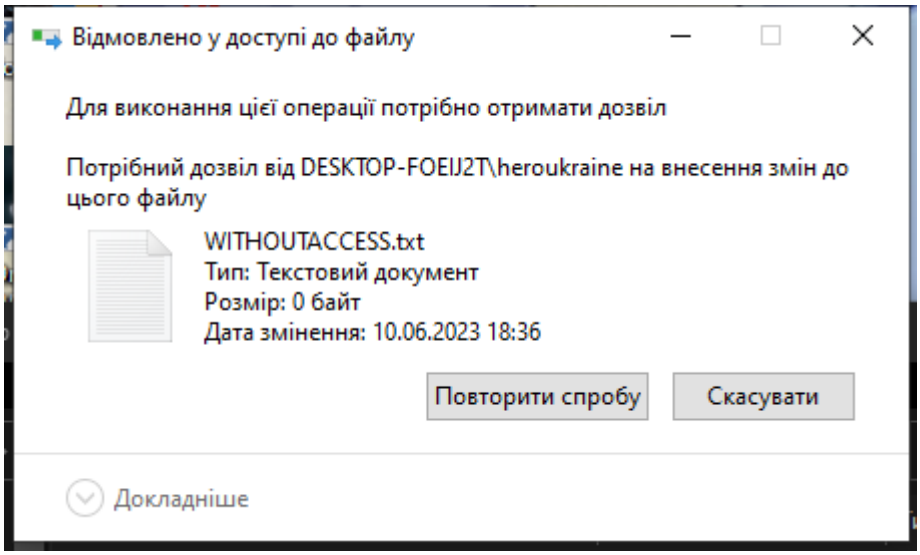


Рисунок 1.33 Повідомлення про відмовлення у видаленні файлу

1.3 Аудит ресурсів і подій системи захисту

В операційній системі Windows 10 існує можливість налаштування аудиту ресурсів і подій, що дозволяє відстежувати події, що відбуваються на комп'ютері, і ресурси, які використовуються користувачами. Аудит ресурсів і подій дозволяє адміністраторам моніторити безпеку системи, виявляти порушення та аналізувати активність.

1.3.1 Налаштування політики аудиту

Вхожу до системи під будь-яким обліковим записом, що входить до групи Адміністратори (Administrators).

Натискаю Пуск (Start), далі Виконати (Run), у полі Відкрити (Open) набираю mmc і натискаю кнопку ОК.

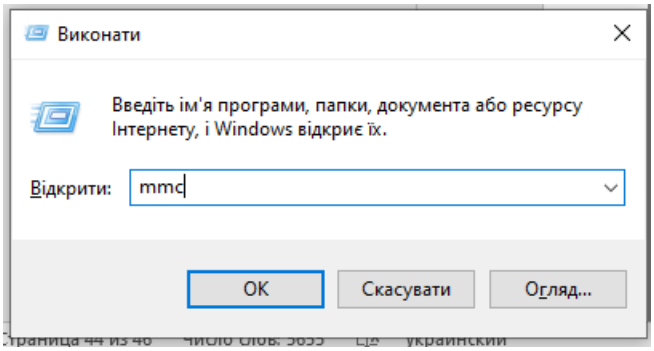


Рисунок 1.34 Відкриття Консолі 1

У вікні Консоль 1 (Console 1), у меню Файл (File), обираю Додати або видалити оснастку (Add/Remove Snap-In).

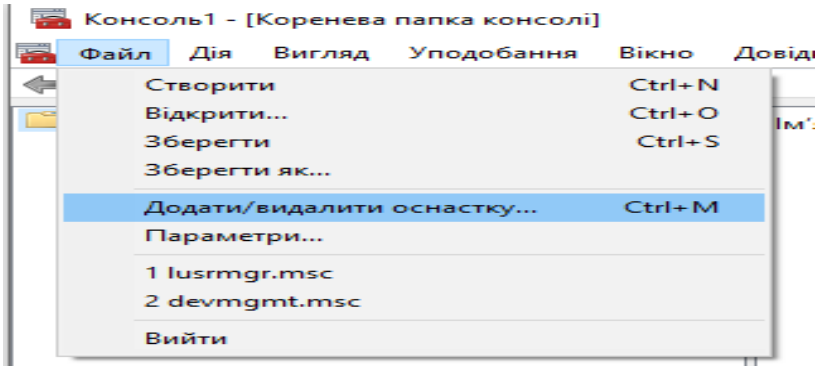


Рисунок 1.35 Меню Файл

У вікні обираю Додати або видалити оснастку (Add/Remove Snap-In)

У діалоговому вікні Додати оснащення (Add Snap-In) обираю у списку оснащення Групова політика (Group Policy) та натискаю Додати (Add).

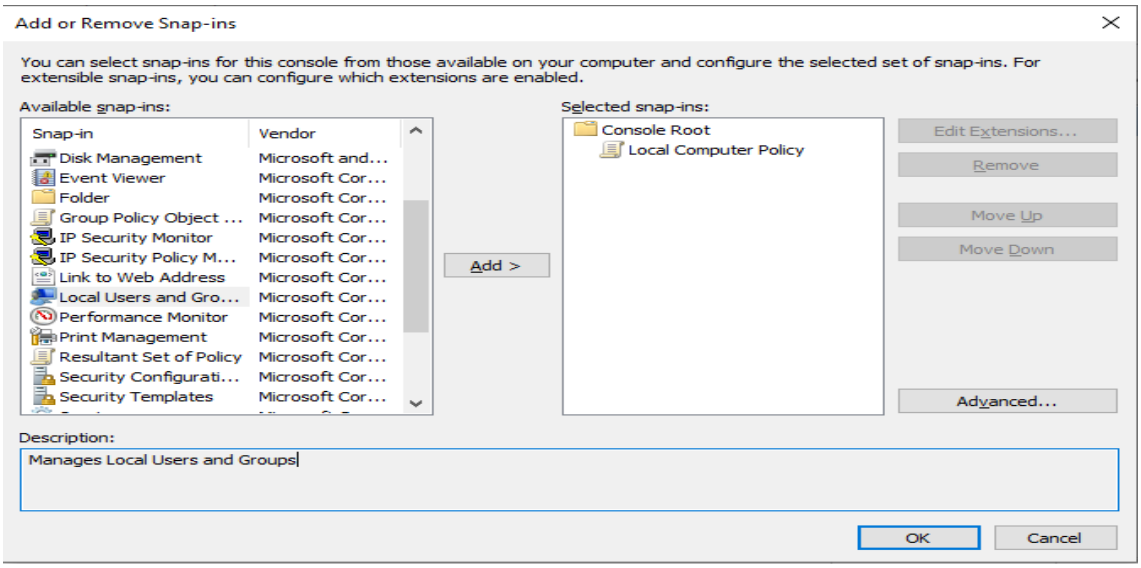


Рисунок 1.36 Вікно Додати або видалити оснастку (Add/Remove Snap-In)

Можна побачити на Рисунку 1.37 , що у вікні Вибрати Ціль відображається елемент Політика «Локальний комп'ютер» (Local Computer Policy) незважаючи на те, що я обрав оснастку Групова політика (Group Policy).

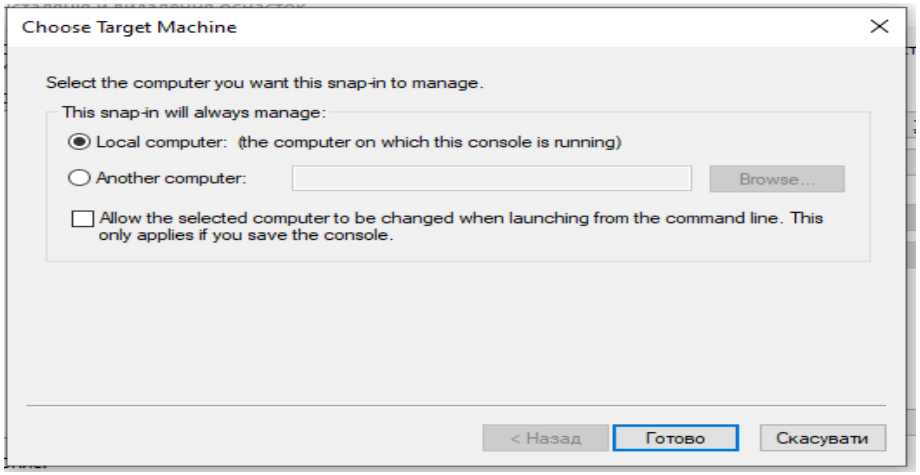


Рисунок 1.37 Вікно Вибрати цільову машину(Choose Target Machine)

Річ у тім, що з локального комп'ютера Групова політика (Group Policy) означає те саме, як і Політика «Локальний комп'ютер» (Local Computer Policy). У дереві консолі переходжу до Політика локального комп'ютера (Local Computer Policy)

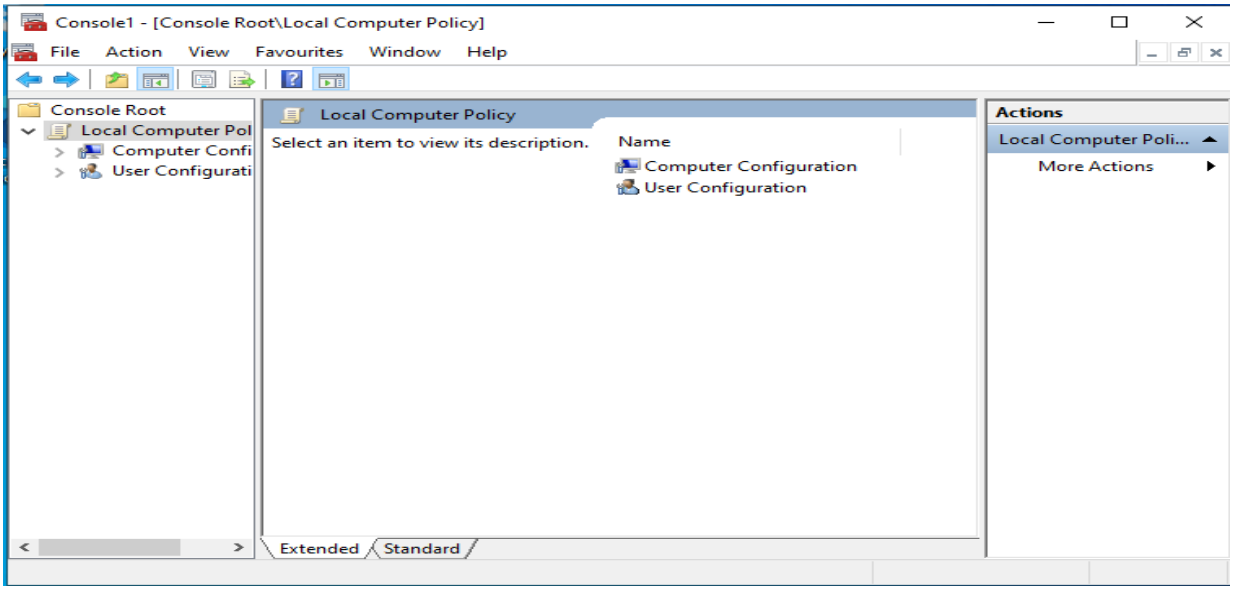


Рисунок 1.38 Вікно Політика локального комп'ютера

Заходжу Конфігурація комп'ютера (Computer Configuration), а потім - Конфігурація Windows (Windows Settings).

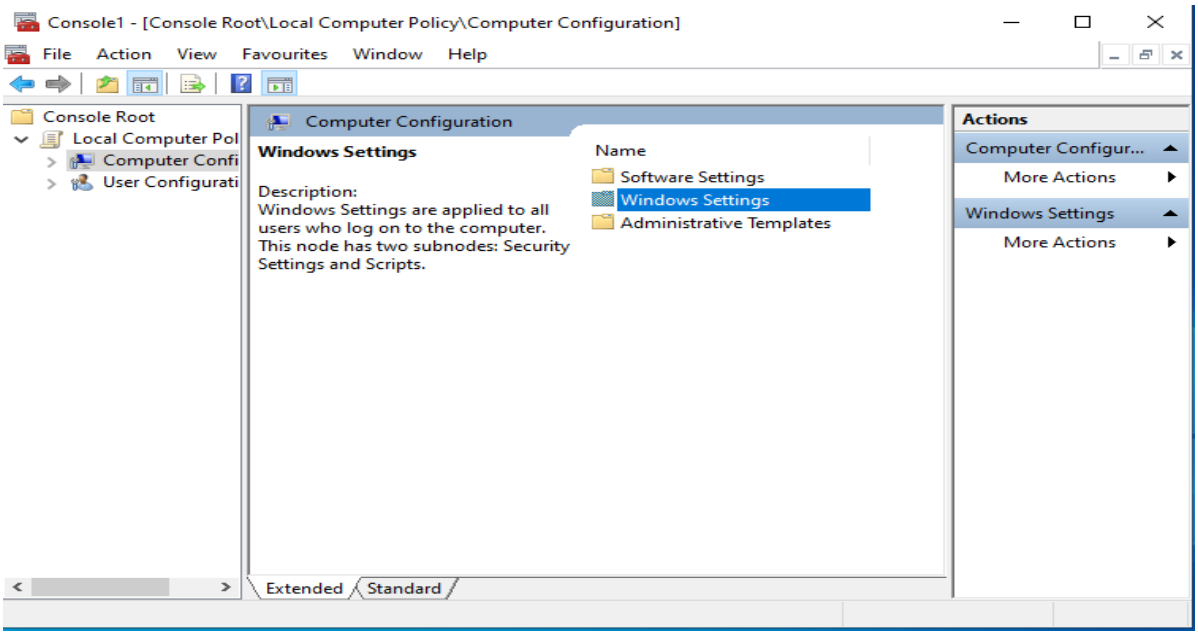


Рисунок 1.39 Вікно Конфігурація комп'ютера

Заходжу в пункт Параметри безпеки (Security Settings).

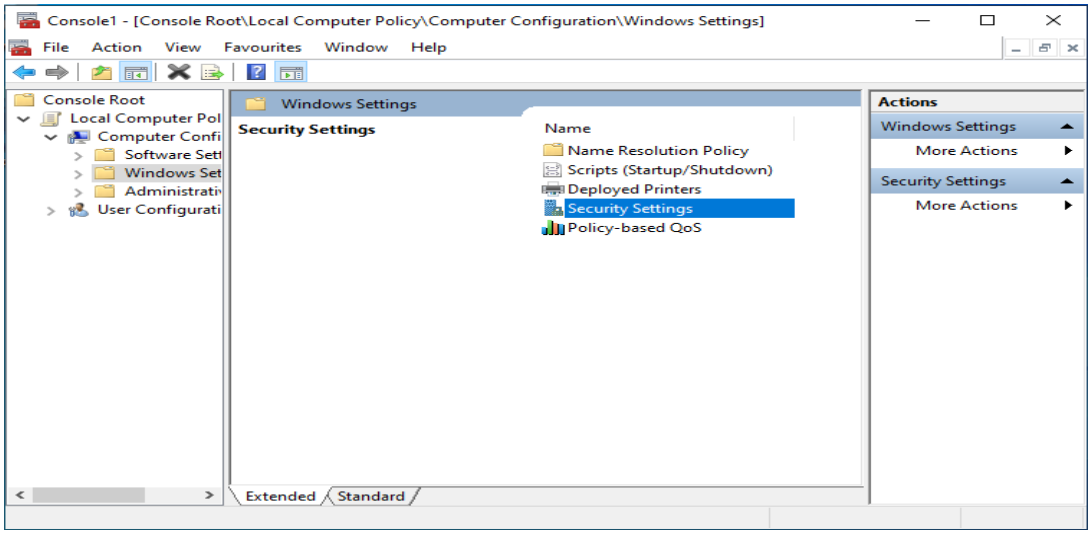


Рисунок 1.39 Вікно Параметри безпеки

Потім переходжу пункт Локальні політики (Local Policies).

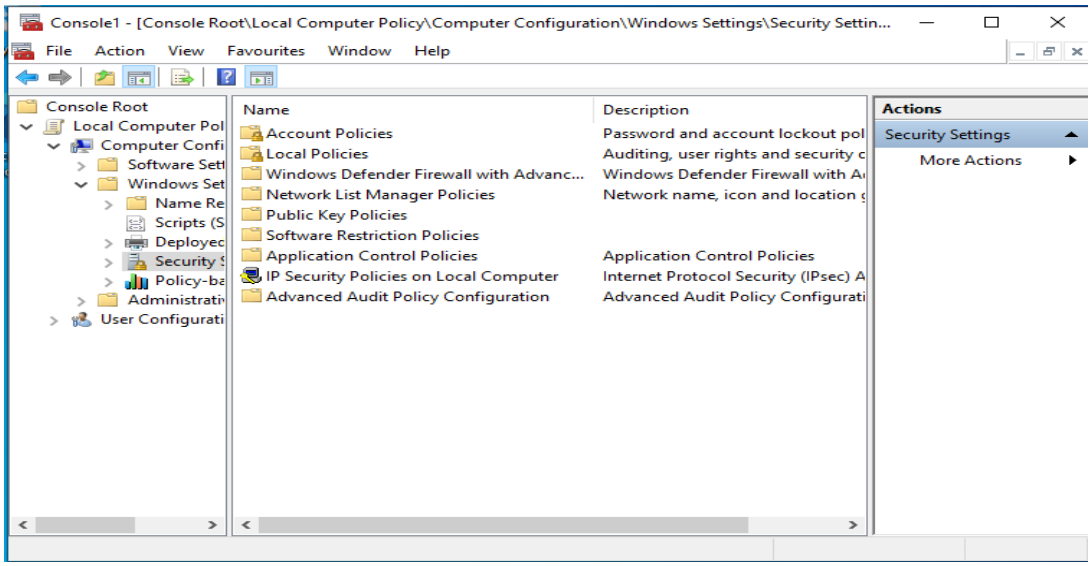


Рисунок 1.40 Вікно Локальні політики

Переходжу у Політика аудиту (Audit Policy). У правій панелі вікна Політика локального комп'ютера (Local Computer Policy) відображаються поточні параметри політики аудиту, як показано в Таблиці 1.3.

Щоб налаштувати політику аудиту, у списку вказую Аудит входу в систему (Audit Logon Events) і в меню Дія (Action) обираю пункт Властивості (Properties), у правій частині вікна обираю кожен тип події і встановлюю

прапорець Успіх (Audit Succes) Attempts) або Відмова (Audit Failed Attempts) згідно з наступною таблицею

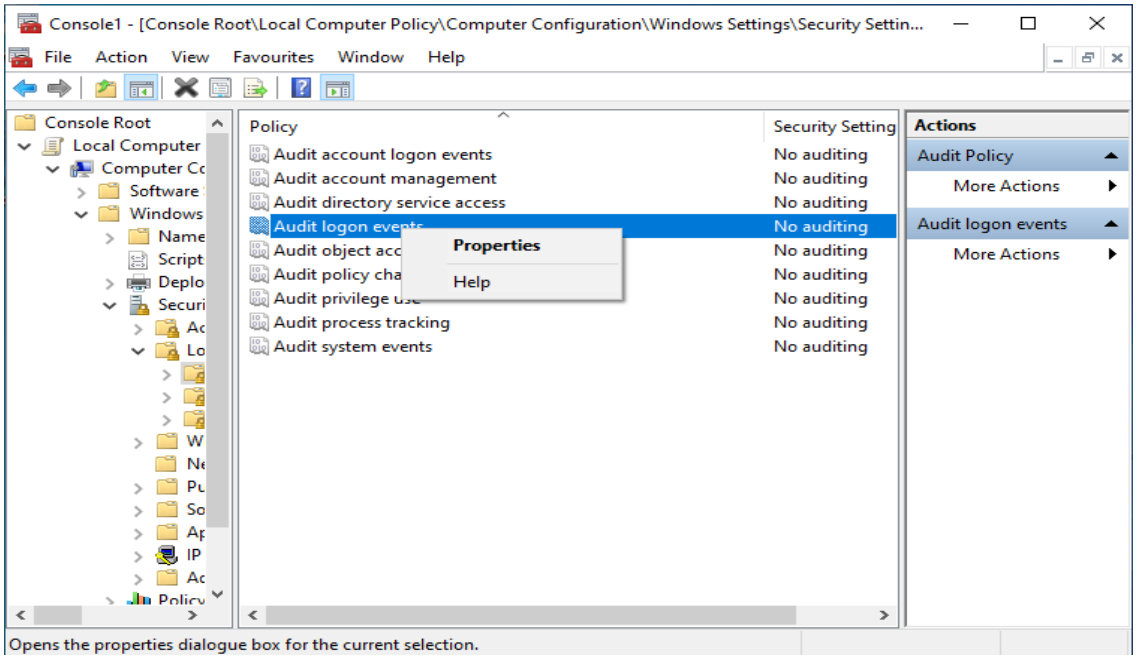


Рисунок 1.41 Вікно для Налаштування політики аудиту

Реєстрована дія	Успіх	Відмова
Події входу до системи		
Управління обліковими записами	X	
Доступ до служби каталогів		
Вхід в систему		X
Доступ до об'єктів	X	X
Зміна системної політики	X	
Використання привілеїв	X	
Відстеження процесу	X	X
Системні події		

Таблиця. 1.3 Поточні параметри політики аудиту

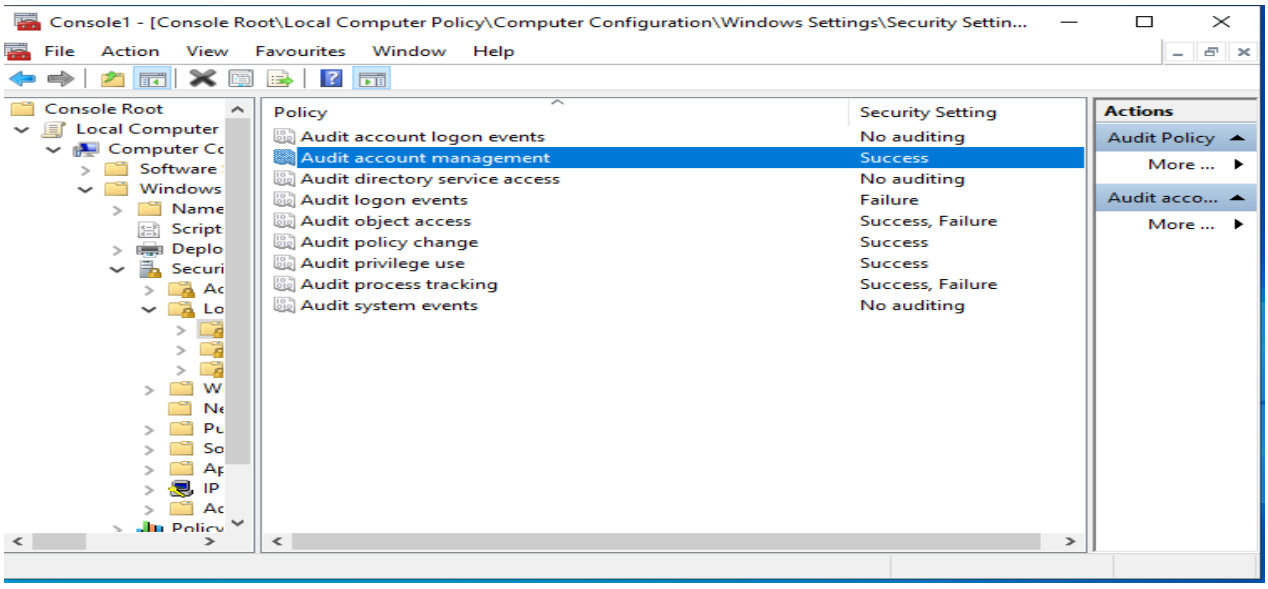


Рисунок 1.42 Налаштовані політики аудиту

14. Закриваю консоль MMC та зберігаю локальну групову політику.

15. Перезапускаю комп'ютер, щоб зміни негайно набули чинності.

Команда gpupdate дозволяє оновлювати параметри як локальної групової політики, так і політики об'єктів Active Directory, включаючи параметри безпеки. Щоб оновити параметри на локальному комп'ютері, входжу у командний рядок, набираю gpupdate і натискаю Enter.

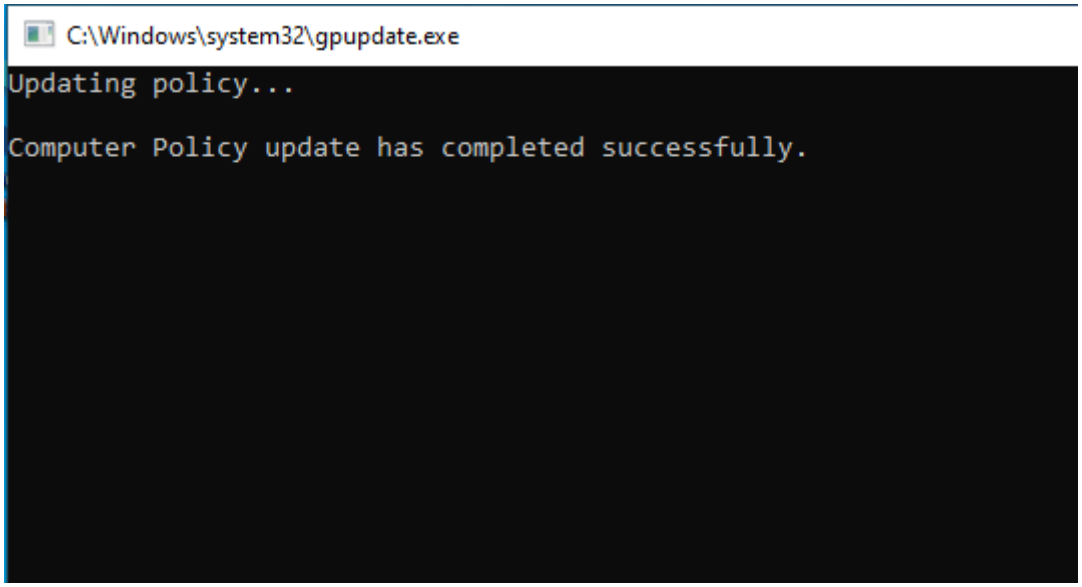


Рисунок 1.43 Командний рядок успішно виконав команду gpupdate

1.3.2 **Аудит об’єктів Windows 10**

В операційній системі Windows 10 існує можливість налаштування аудиту об'єктів, що дозволяє відстежувати події та дії, які відбуваються на комп'ютері.

Аудит об'єктів може бути корисним для моніторингу безпеки системи, виявлення вразливостей або ненормальної активності.

Налаштування аудиту файлів

1. Входжу до системи за допомогою будь-якого облікового запису, що входить до групи Адміністратори (Administrators).

2. За допомогою Провідника (Windows Explorer) створюю папку з ім'ям Audit у корені системного диска

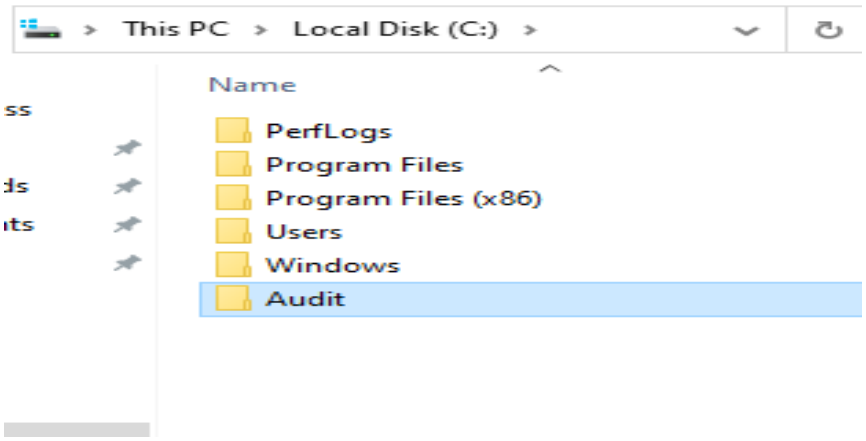


Рисунок 1.44 Папка Audit

3. У папці Audit створюю текстовий файл під назвою AUDIT (наприклад, C:\Audit\Audit).

4. Переходжу у Властивості (Properties) файла AUDIT.

5. У діалоговому вікні Властивості (Properties) обираю вкладку Безпека (Security) і натискаю кнопку Додатково (Advanced). Щоб вимкнути простий доступ до файлів, заходжу в Пуск (Start), далі -Мій комп'ютер (My Computer), потім перехеоджу в меню Провідник (Explore). У меню Сервіс (Tools) обираю пункт Властивості папки (Folder Options).

На вкладці Вигляд знімаю прапорець Use Sharing Wizard(Recommended) і натискаю кнопку ОК.

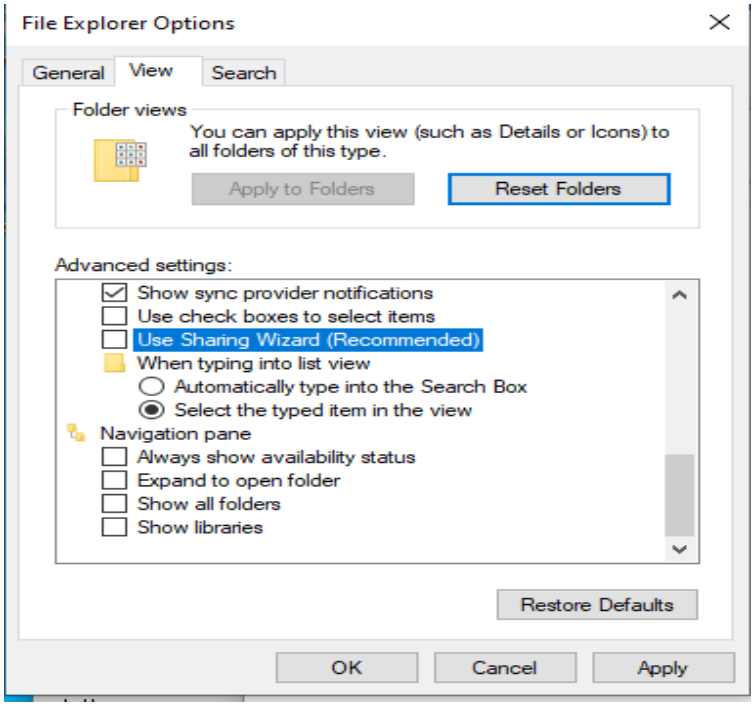


Рисунок 1.45 Вікно File Explorer Options

6. У діалоговому вікні Додаткові параметри безпеки для AUDIT обираю вкладку Аудит (Auditing).

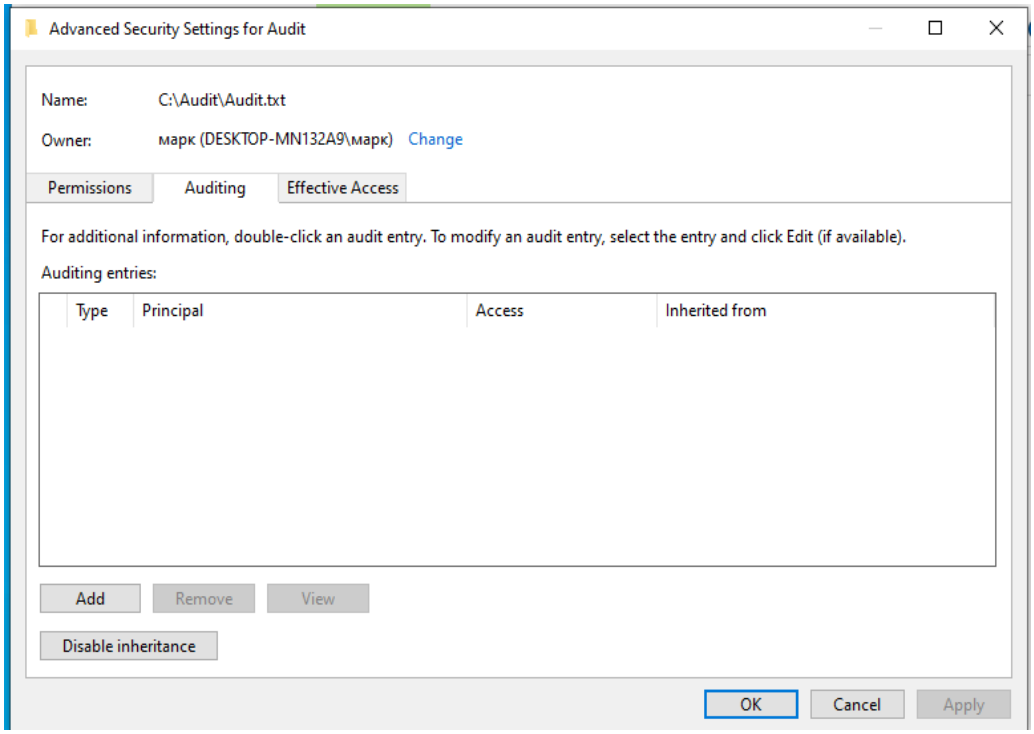


Рисунок 1.46 Advanced Settings for Audit

7. Натискаю кнопку Додати (Add). В діалоговому вікні Вибір: користувач або група (Select User Or Group), в поле Ім’я (Name), вказую Все (Everyone) і ОК. У діалоговому вікні Елемент аудиту для Audit.txt (Audit Entry For Audit.txt) встановіть прапорці Успіх (Successful) та Відмова (Failed) для кожної з наступних подій:

- Створення файлів/Запис даних (Create Files/Write Data).
- Видалення (Delete).
- Зміна дозволів (Change Permissions).
- Зміна власника (Take Ownership).

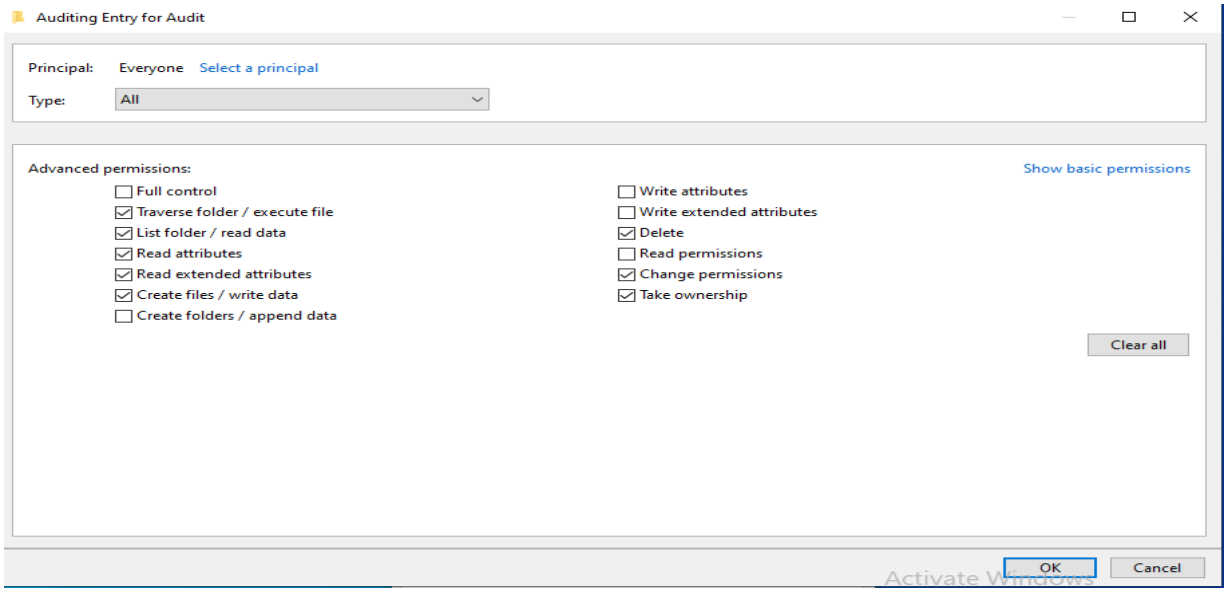


Рисунок 1.47 Налаштування прав Аудиту

Натискаю кнопку ОК. Windows 10 відобразить групу Усі (Everyone) у діалоговому вікні Додаткові параметри безпеки для audit.txt (Advanced Security Settings For).

Перевірка правильності параметрів політики аудиту для файлу AUDIT

1. Натискаю кнопку Пуск (Start), Панель керування (Control Panel), потім — Облікові записи користувачів (User Accounts).

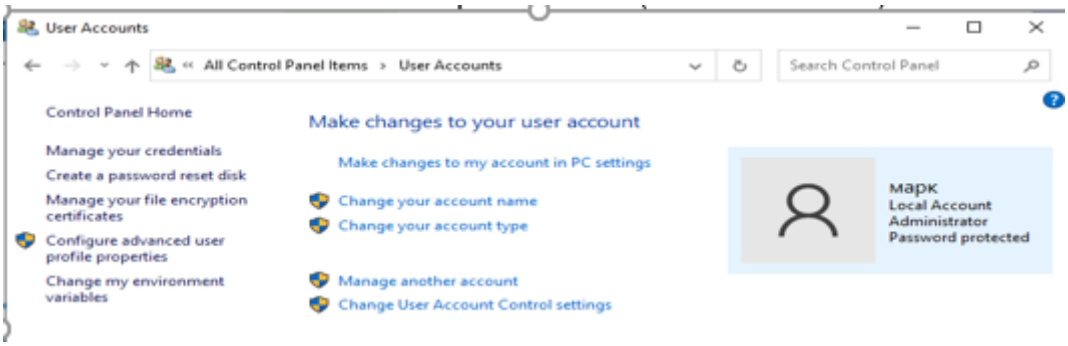


Рисунок 1.48–

2. Переконуюсь, що обліковий запис User2 існує і обмежений (Limited).

3. Створюю пароль User2 для облікового запису User2.

4. Виходжу із системи.

5. Змінюю обліковий запис User2, використовуючи пароль.

6. Відкриваю Провідник (Windows Explorer), а потім відкриваю файл C:\Audit\Audit. У вікні програми Блокнот (Notepad) з'явиться порожній файл AUDIT

7. Вводжу наступний текст: «Цей файл змінено користувачем User2». Але зберігти його не вдається , бо доступ до зміни файлу нема.

8. Закриваю файл, не зберігаючи його, та завершую роботу із системою.

1.3.3 **Керування журналом безпеки**

Перегляд журналу безпеки комп'ютера та відбору подій Намагаюся увійти до User 2, навмисно використовуючи неправильний пароль, декілька разів. Я це роблю для того , щоб це відобразилося у журналі безпеки. Далі входжу до системи під будь-яким обліковим записом, що входить до групи Адміністратори (Administrators).

Переходжу у Пуск (Start), Панель керування (Control Panel).

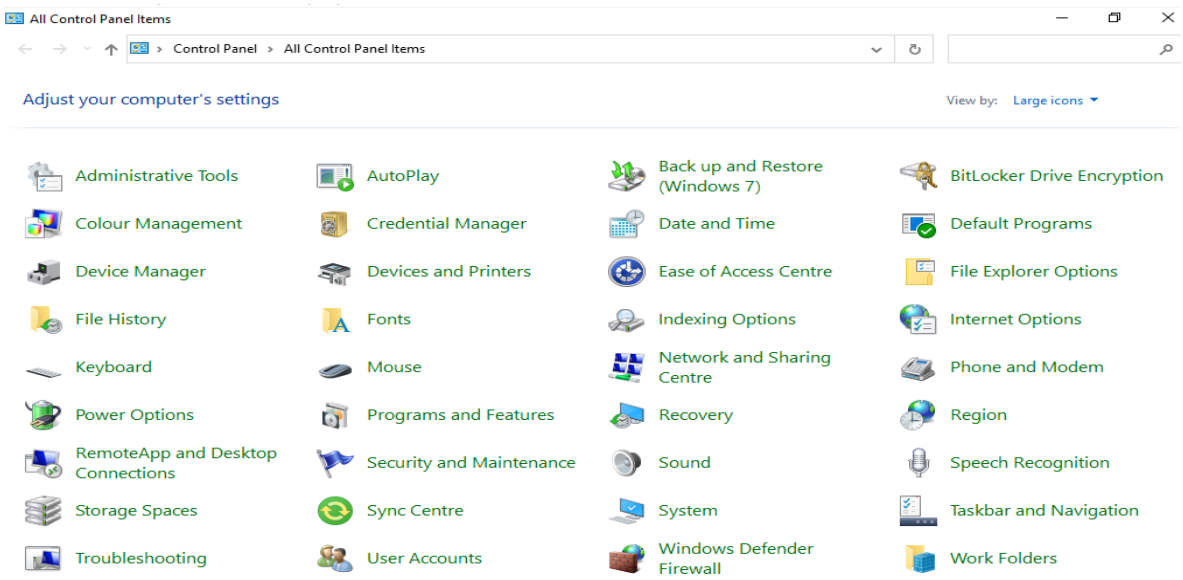


Рисунок 1. Вікно Панель керування

Далі у категорію Адміністрація (Administrative Tools).

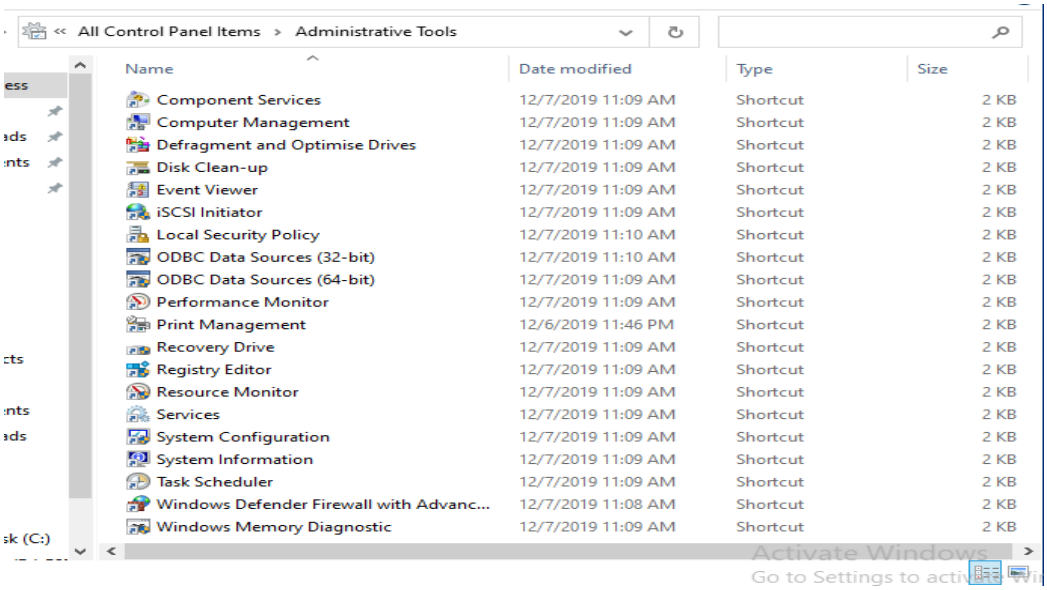


Рисунок 1. Вікно Адміністрація (Administrative Tools).

Потім у Перегляд подій (Event Viewer)

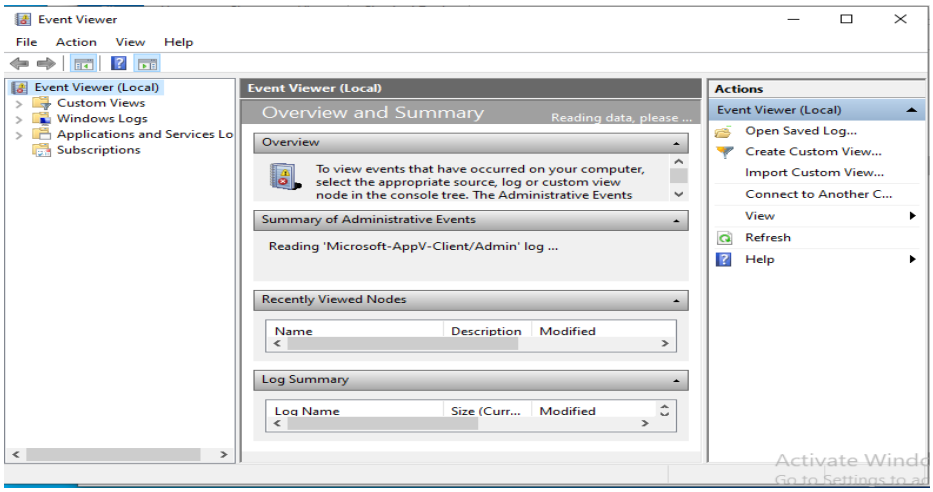


Рисунок 1. Вікно Перегляд подій

У дереві консолі заходжу у програму (Application Log) і переглядаю її зміст. Переглядаю опис кількох подій, заходячи у відповідні записи.

У дереві консолі обираю система (System Log) та переглядаю його вміст.

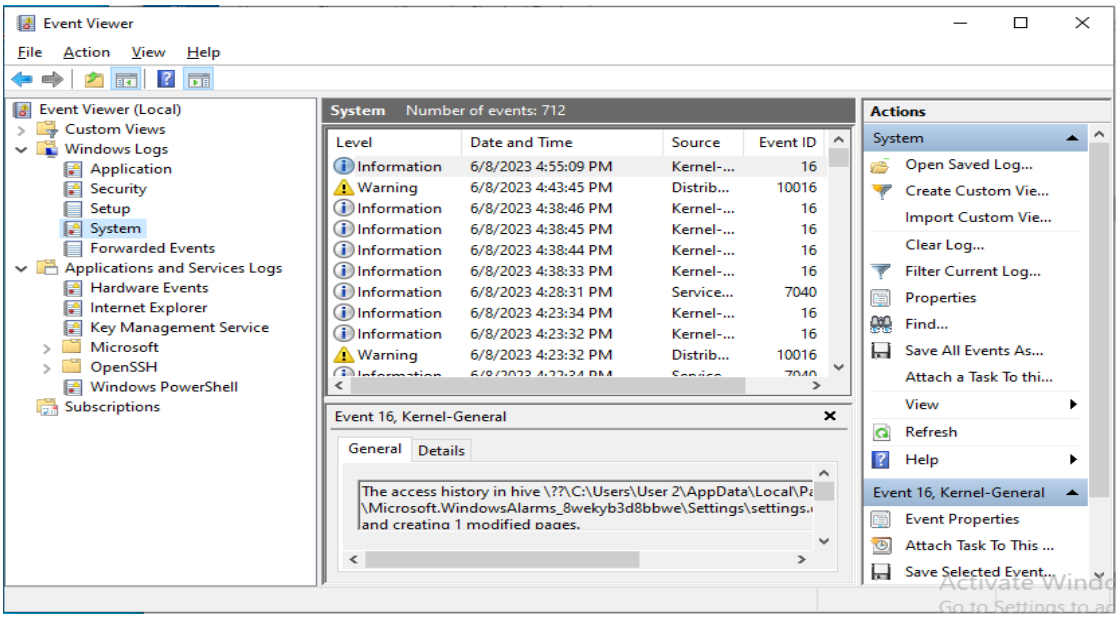


Рисунок 1. Вікно Перегляд подій з подіями в системі

Переглядаю опис кількох подій і кожну їх дію відповідних записів. У колонці Категорія (Category) відображається тип події, наприклад доступ до об'єкта, керування обліковими записали, доступ до служби каталогів або спроби реєстрації в системі. Щоб переглянути додаткову інформацію про будь-яку подію, обираю назву події та в меню Дія (Action) , а далі заходжу у Властивості (Properties).

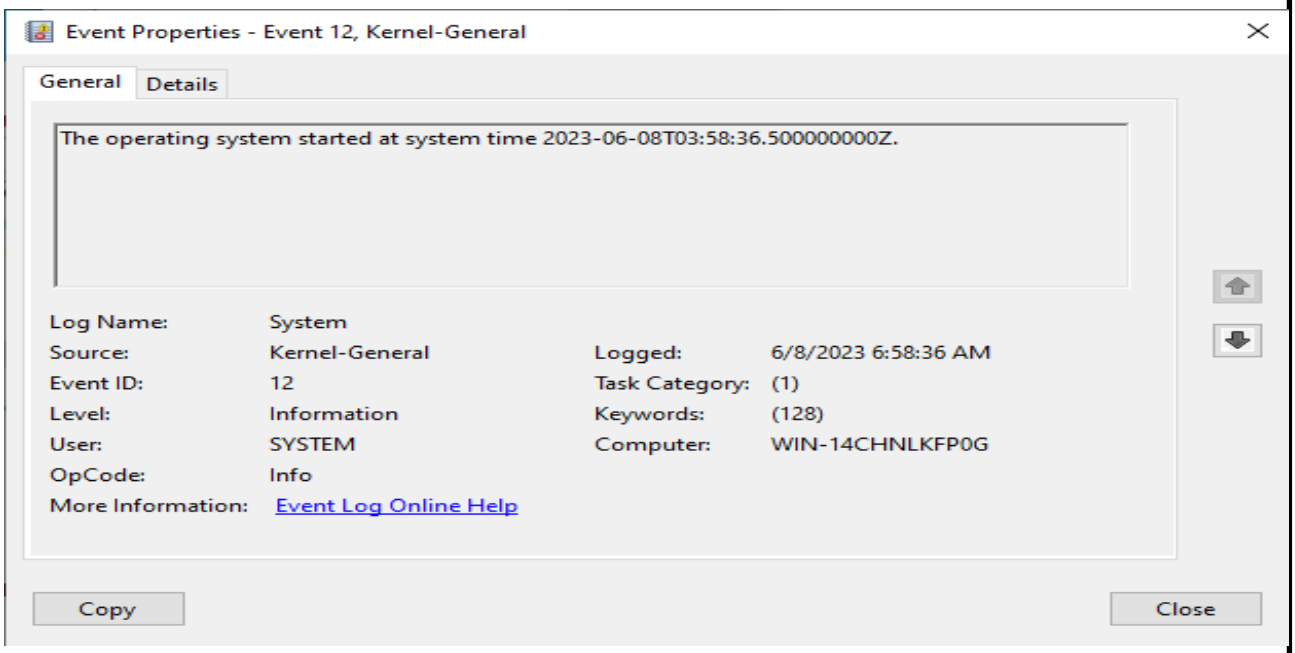


Рисунок 1. Вікно з властивостями вибранної події

У дереві консолі знаходжу безпеку (Security Log) та переглядаю її вміст. Успішні спроби умовно позначені значком ключа, а невдалі – значком замка.

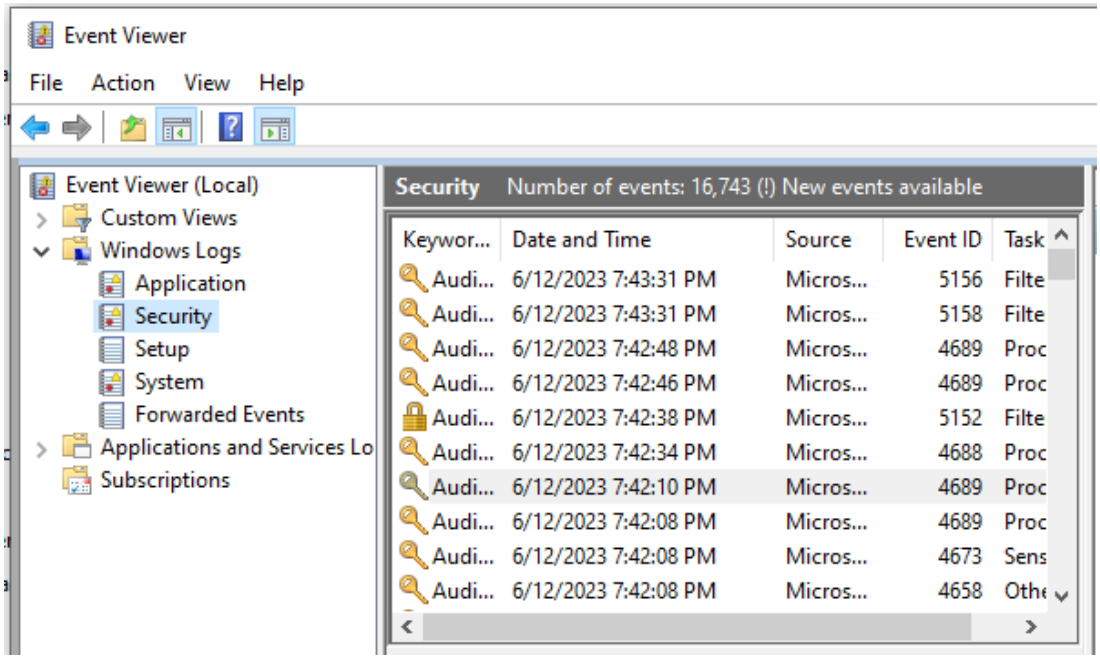


Рисунок 1. Вікно Перегляду подій, де вказані спроби увійти в систему

Крім того, вказані дата та час події, категорія події та користувач, дія якого викликала цю подію. Тут можна побачити те, що робив я до цього, а саме ,намагався увійти з неправильним паролем.

У меню Вигляд обираю пункт Фільтр.

У діалоговому вікні Властивості: Система (System) у полі Користувач (User) ввожу User2 і ОК. Застосування фільтра зменшить кількість подій, які доведеться переглянути, щоб знайти потрібне.

Переглядаю кожну подію. Можна побачити, що всі вони відносяться до користувача User2.

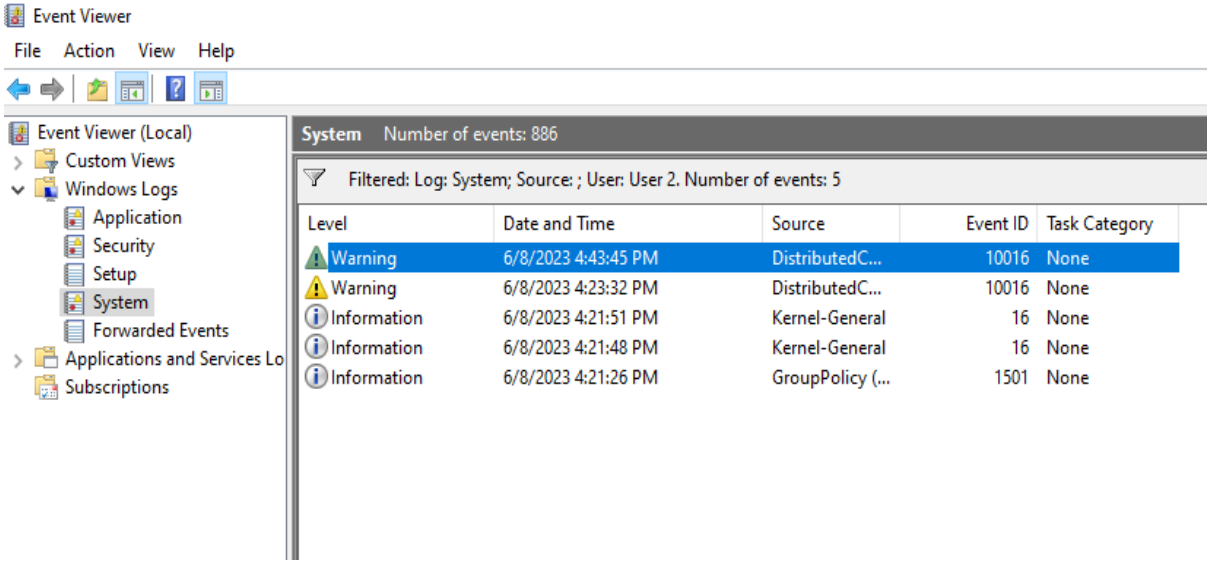


Рисунок 1.55 Застосований фільтр для перегляду подій користувача User2

Таким чином , завдяки Перегляд подій , можна дивитися аудит системи з користувачами.

Налаштування розміру та вмісту файлу журналу

1. У дереві консолі обираю пункт Система (System).

2. У меню Дія (Action) переходжу у Властивості (Log Properties).

3. У діалоговому вікні властивостей журналу обираю Затирати старі події (Overwrite Events As Needed)

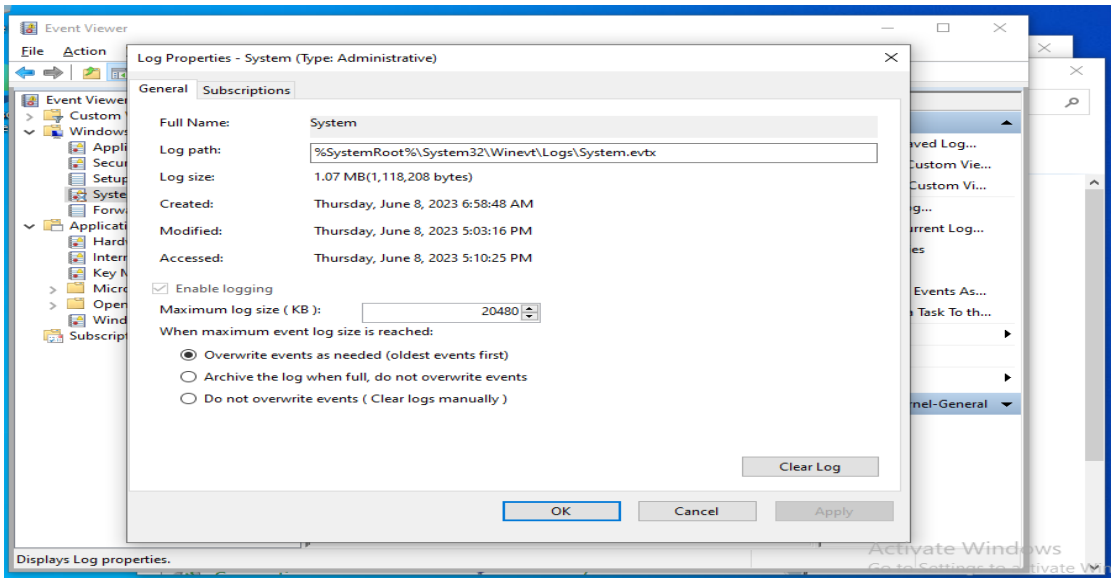


Рисунок 1. Вікно Log Properties

4. У полі Максимальний розмір журналу (Maximum Log Size) змінюю максимальний розмір журналу на 2048 кбайт і натискаю кнопку ОК. Тепер Windows 10 буде заповнювати журнал, доки його обсяг не досягне 2048 кбайт, а потім почне затирати старі події за необхідності.

5. Закриваю вікно Перегляд подій (Event Viewer) та вікно Адміністрування (Administrative Tools).

1.4 СТВОРЕННЯ БАЗОВОЇ КОНФІГУРАЦІЇ БЕЗПЕКИ WINDOWS

1.4.1 "Політика облікових записів"

"Політика облікових записів" (Account Policy) є засобом у Windows, який дозволяє налаштовувати параметри безпеки для облікових записів користувачів. Для доступу до "Політики облікових записів" потрібно виконати наступні кроки:

1.Відкриваю "Панель управління" (Control Panel).

2.Обираю "Адміністрування" (Administration)

У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).

Потім обираю "Політика облікових записів" (Account Policy).

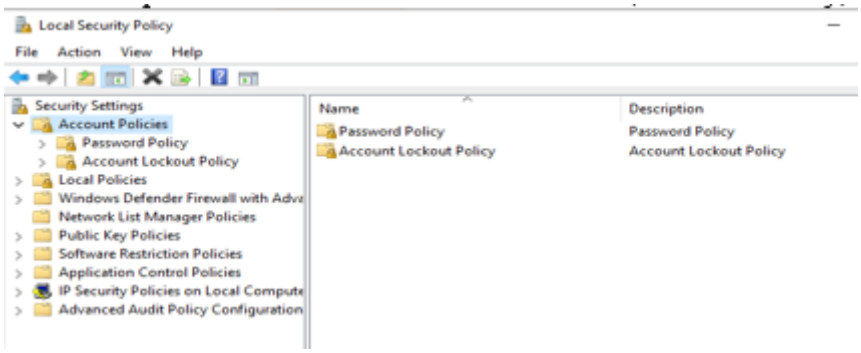


Рисунок Вікно Account Policies

В "Політиці облікових записів" можна налаштовувати такі параметри безпеки:

1. Політика складності паролів:

- Мінімальна довжина пароля: Встановлення мінімальної кількості символів, яку має мати пароль.
- Вимагати використання різних типів символів: Встановлення вимоги до використання різних типів символів у паролі (наприклад, букви верхнього та нижнього регістру, цифри, спеціальні символи).
- Вимагати періодичну зміну пароля: Встановлення інтервалу, через який користувачеві потрібно змінити свій пароль.

2. Блокування облікових записів:

- Максимальна кількість невдалих спроб входу: Встановлення максимальної кількості невдалих спроб введення пароля перед блокуванням облікового запису.
- Тривалість блокування облікового запису: Встановлення тривалості блокування облікового запису після досягнення максимальної кількості невдалих спроб.

3.Політика життєвого циклу паролів:

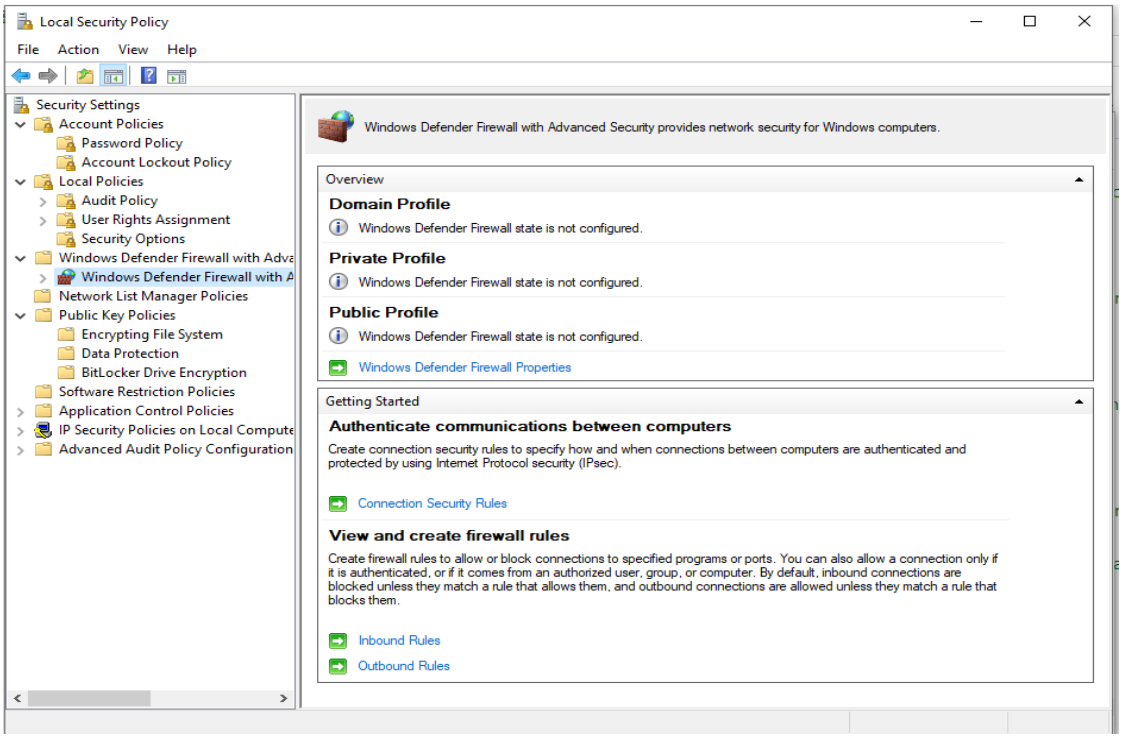
- Максимальний термін дії пароля: Встановлення максимального часового періоду, після якого користувачев

1.4.2 **Засіб "Брандмауер Windows у режимі підвищеної безпеки"**

Засіб "Брандмауер Windows у режимі підвищеної безпеки" (Windows Firewall with Advanced Security) є засобом безпеки в операційній системі Windows, який надає розширені можливості для керування мережевим трафіком і захисту вашої системи.

Цей засіб дозволяє вам налаштовувати правила брандмауера, контролювати вхідний і вихідний мережевий трафік та забезпечувати безпеку вашої системи. Для доступу до "Брандмауера Windows у режимі підвищеної безпеки" виконую наступні кроки:

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration)
3. У цьому розділі знаходжу та обираю "Брандмауер Windows у режимі підвищеної безпеки" (Windows Firewall with Advanced Security).



Рисунок

Після відкриття "Брандмауера Windows у режимі підвищеної безпеки" ви можете налаштовувати наступні параметри безпеки:

1. Правила вхідного трафіку:
    - Дозволити чи заборонити певний вхідний трафік на основі портів, протоколів, програм або IP-адрес.
    - Встановити правила для блокування небажаного або потенційно шкідливого вхідного трафіку.
2. Правила вихідного трафіку:
    - Дозволити чи заборонити певний вихідний трафік на основі портів, протоколів, програм або IP-адрес.
    - Керувати вихідним трафіком для запобігання несанкціонованому передачі даних з вашої системи.
3. Доменні профілі брандмауера:
    - Налаштування брандмауера для роботи в доменній мережі.
4. Приватні профілі брандмауера:
    - Налаштування брандмауера для роботи в приватній мережі (наприклад, домашній мережі).
5. Публічні профілі брандмауера:
    - Налаштування брандмауера для роботи в публічній мережі (наприклад, громадській Wi-Fi мережі).
6. Захист від інтранет-атак:
    - Налаштування захисту вашої системи від потенційних атак з інтранету.
    -

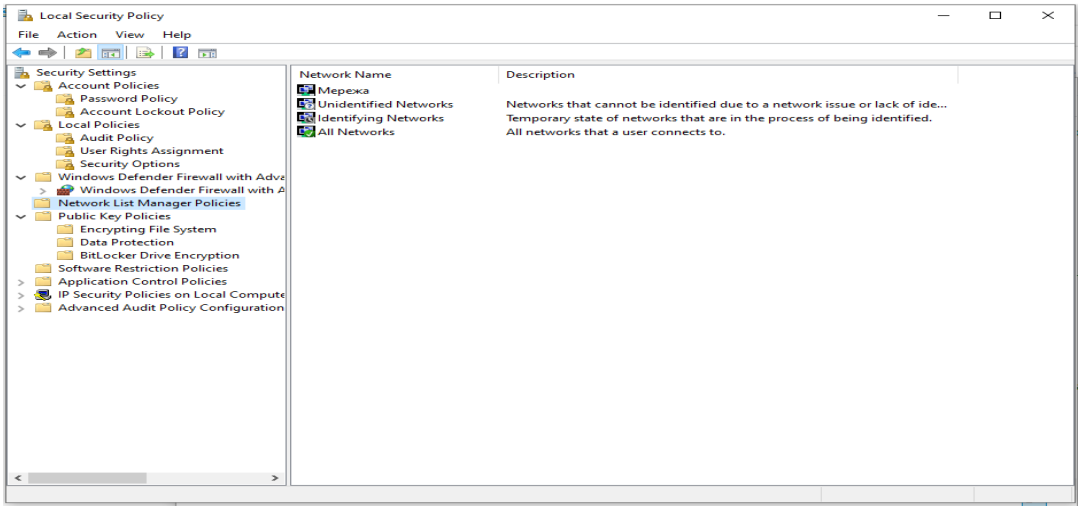
1.4.3 **Засіб "Політики диспетчера списку мереж"**

Засіб "Політики диспетчера списку мереж" (Network List Manager Policies) в Windows дозволяє налаштовувати політики, пов'язані з управлінням списком мереж, до яких ваш комп'ютер підключається. Цей засіб дозволяє вам

контролювати поведінку вашої системи щодо різних типів мереж, таких як доменні, приватні та публічні мережі.

Для доступу до "Політик диспетчера списку мереж" виконую такі кроки:

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration) .
3. У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).
4. Розгортаю розділ "Політики безпеки локального комп'ютера" (Local Policies) і переходжу до "Політик диспетчера списку мереж" (Network List Manager Policies).



Рисунок

У "Політиках диспетчера списку мереж" ви можете налаштовувати наступні параметри:

1. Профіль мережі:
    - Встановити тип профілю (доменний, приватний або публічний) для кожної мережі.
    - Керувати автоматичною зміною профілю при підключенні до нової мережі.
2. Налаштування приватних мереж:

- Встановити політику для приватних мереж, таких як дозволити файли та принтери, дозволити відкритий мережевий доступ, дозволити автоматичну настроювання мережі і т. д.

3. Налаштування публічних мереж:
    - Встановити політику для публічних мереж, таких як блокування файлив і принтерів, обмеження мережевого доступу і т. д.
4. Налаштування мереж домена:
    - Встановити політику для мереж домена, таких як дозволити файли та принтери, дозволити робочу групу, дозволити автоматичну настроювання мережі і т. д.
    -

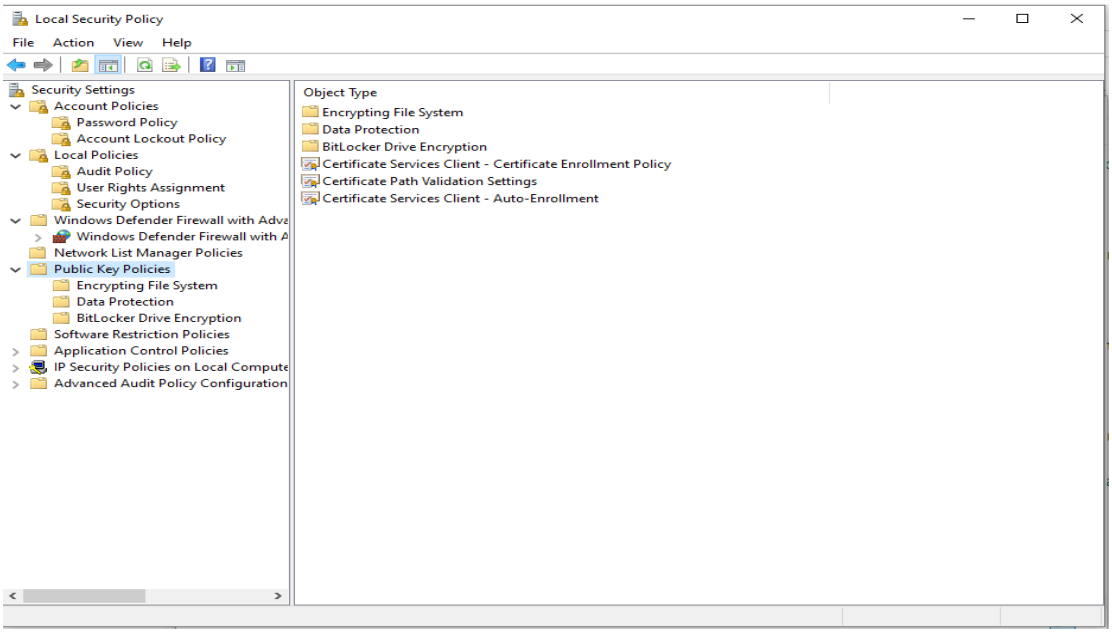
1.4.4 **Засіб "Public Key Policies"**

Засіб "Public Key Policies" (Політики відкритого ключа) в операційній системі Windows використовується для керування і налаштування політик, пов'язаних з використанням відкритих ключів і сертифікатів у системі.

Ці політики дозволяють контролювати використання шифрування, цифрових підписів, аутентифікації та інших криптографічних функцій, пов'язаних з відкритими ключами.

Для доступу до " Політики відкритого ключа " виконую такі кроки:

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration)
3. У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).
4. Потім обираю "Public Key Policies"



Рисунок

У "Public Key Policies" ви зможете налаштовувати різні політики, пов'язані з використанням відкритих ключів, такі як налаштування криптографічних алгоритмів, обмеження довіри до сертифікатів, управління ключами шифрування та цифрових підписів і багато іншого.

Важливо зазначити, що доступ до "Public Key Policies" може вимагати певних привілеїв адміністратора або доступу до групової політики, залежно від конфігурації вашої системи.

1.4.5 **Засіб "Політики обмеженого використання програм"**

Засіб "Політики обмеженого використання програм" (AppLocker) в операційній системі Windows дозволяє налаштовувати політики безпеки, що обмежують використання програм в системі. Цей засіб дозволяє адміністраторам обмежувати, які програми можуть запускатися на комп'ютері або на певному користувачі.

У "Політиках обмеженого використання програм" ви можете налаштовувати наступні параметри:

1. Правила виконання:
    - Визначення правил, які обмежують виконання конкретних програм або файлів на основі шляху, виду файлу, виду виконання і т. д.
    - Налаштування дозволів або заборон на виконання програм для різних груп користувачів або комп'ютерів.
2. Правила скриптів:
    - Визначення правил, які обмежують виконання скриптів на основі шляху, виду файлу, виду виконання і т. д.
    - Налаштування дозволів або заборон на виконання скриптів для різних груп користувачів або комп'ютерів.
3. Правила пакетів програмного забезпечення:
    - Визначення правил, які обмежують виконання пакетів програмного забезпечення на основі виду пакета, виду виконання, власника пакета і т. д.
    - Налаштування дозволів або заборон на виконання пакетів програмного забезпечення для різних груп користувачів або комп'ютерів.

Зміна дозволів та заборона доступу користувачу завдяки засобу AppLocker

1. Відкриваю "Панель управління" (Control Panel).

2. Обираю "Адміністрування" (Administration).

3. У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).

4. Розгортаю розділ "Політики безпеки локального комп'ютера" (Local Policies) і переходжу до "Політик обмеженого використання програм" (AppLocker).

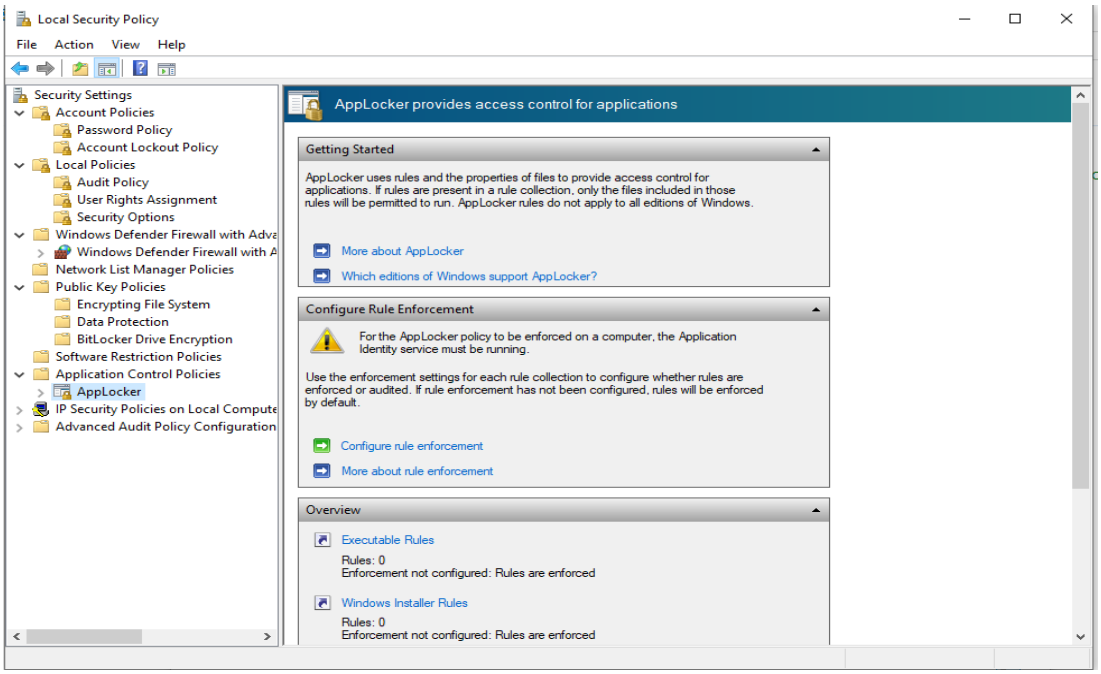


Рисунок 1. Вікно з засобом “AppLocker”

5. Далі переходжу Configure rule enforcement , ставлю прапорець на Executable rules і ОК , щоб застосувати

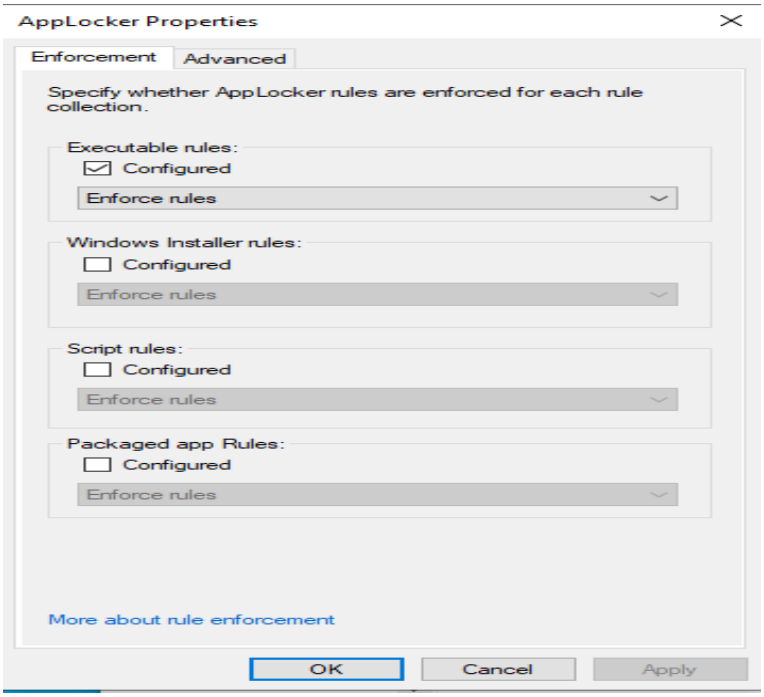


Рисунок 1. Вікно “AppLocker Properties”

6 Далі обираю “Automatically Generate rules

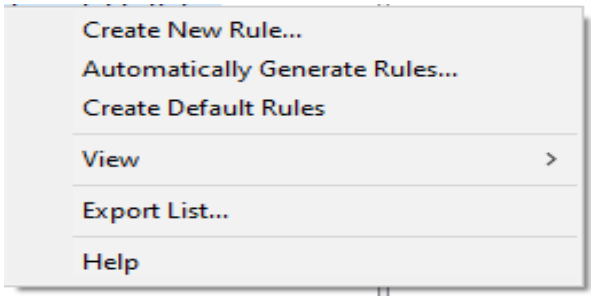
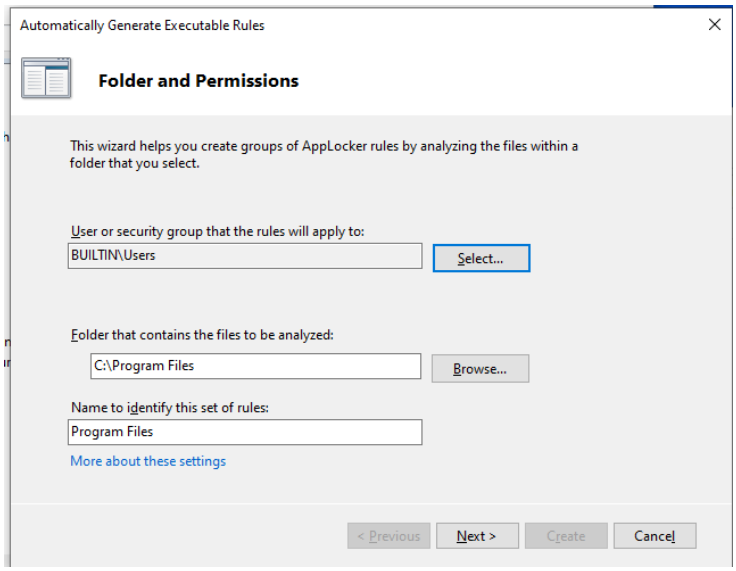


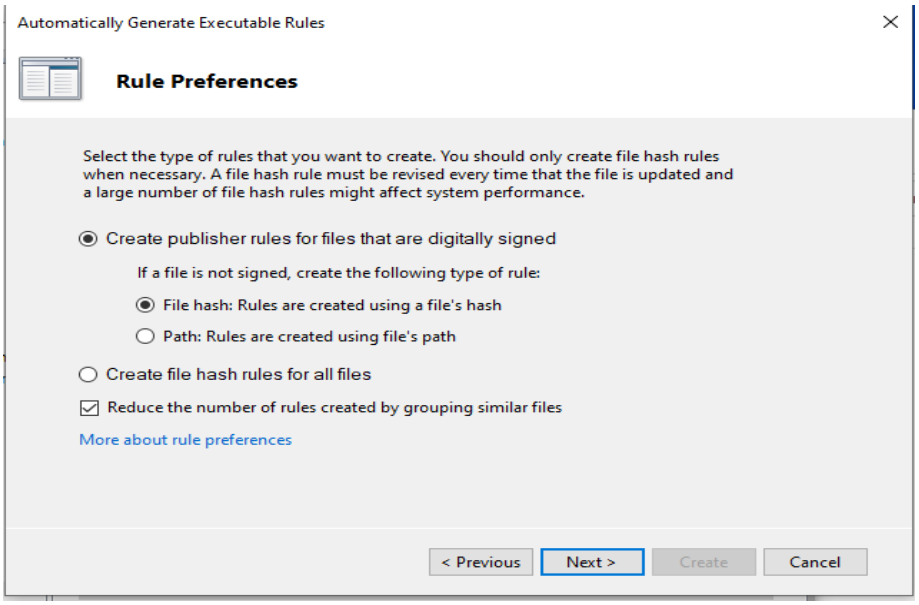
Рисунок 1. Меню для “Executable rules”

7 Після того ,як відкриється вікно Automatically Generate Executable rules, у вкладці “Users or security group that rules will aply to:”обираю Users і натискаю ОК, після чого натискаю Next



Рисунок

8 На наступному вікні також натискаю Next



Рисунок

9 Після чого можна побачити скільки згенерується правил для папки C:\Program Files

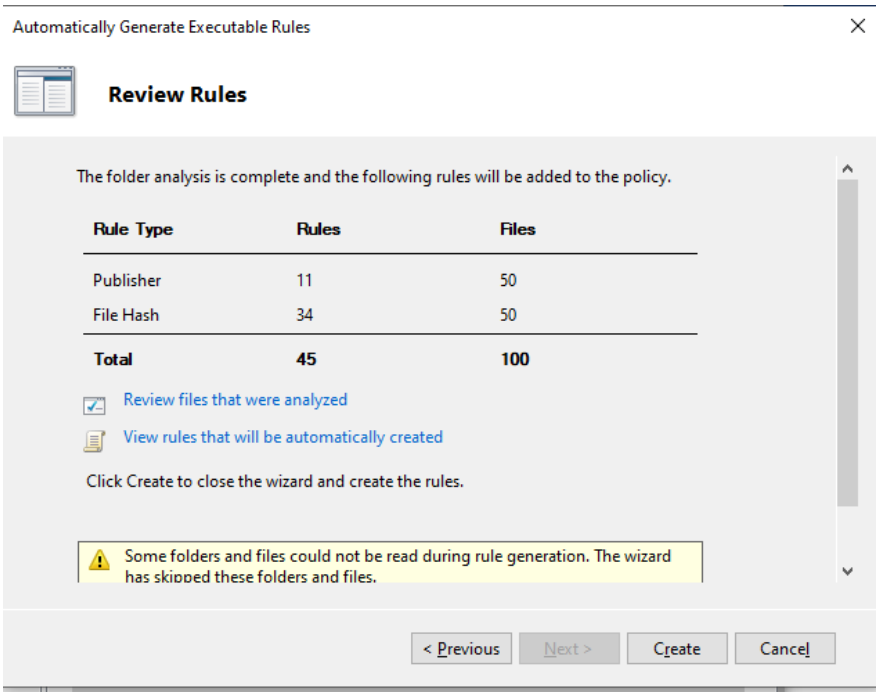


Рисунок 1. Кількість правил автоматично створених правил

10 Натискаю Create і бачу табличку з усіма правилами Рисунок 1.

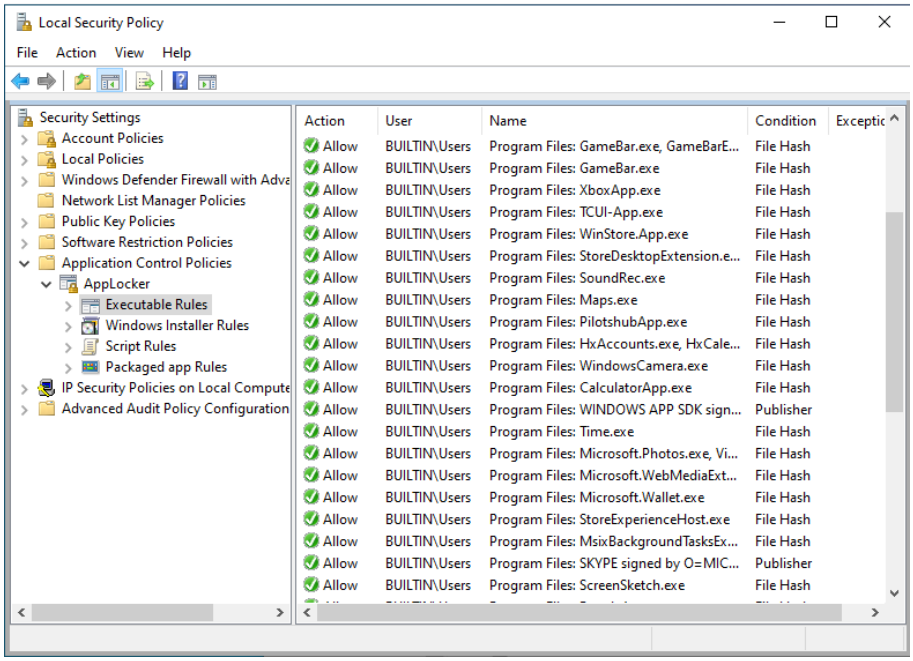


Рисунок 1. Автоматично сгенеровані правила

10 Обираю All programs і заходжу в Properties. Ставлю прапорець на Deny і натискаю ОК.

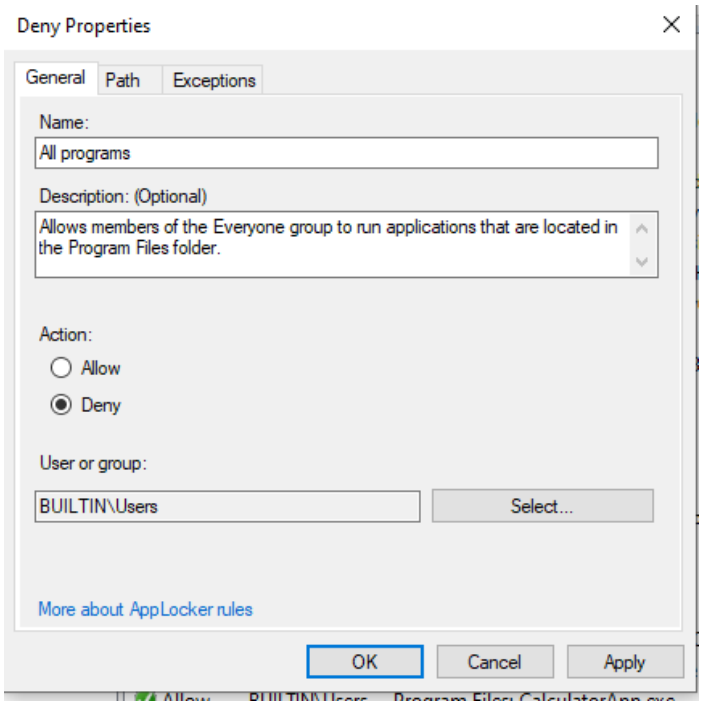


Рисунок 1. Deny properties

11 Після чого змінюю обліковий запис на User 2 і намагаюся запустити Microsoft Edge, але мені це не вдається і з’являється вікно з попередженням.

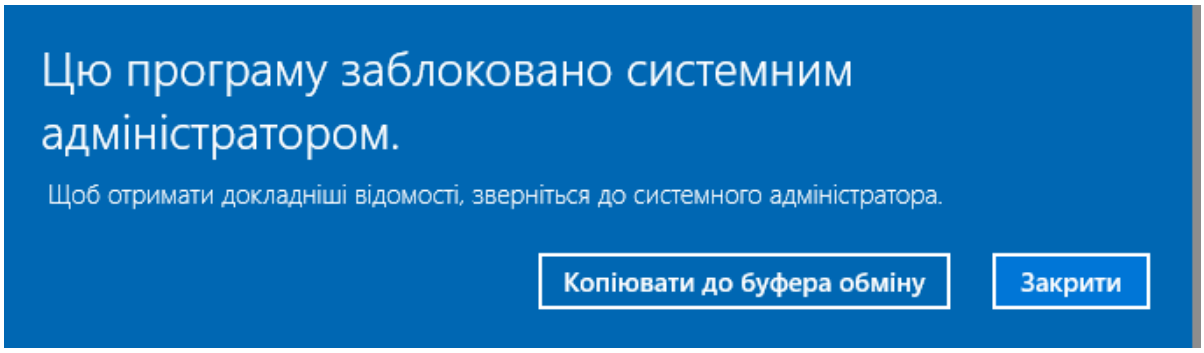


Рисунок 1. Попередження про заблоковану програму.

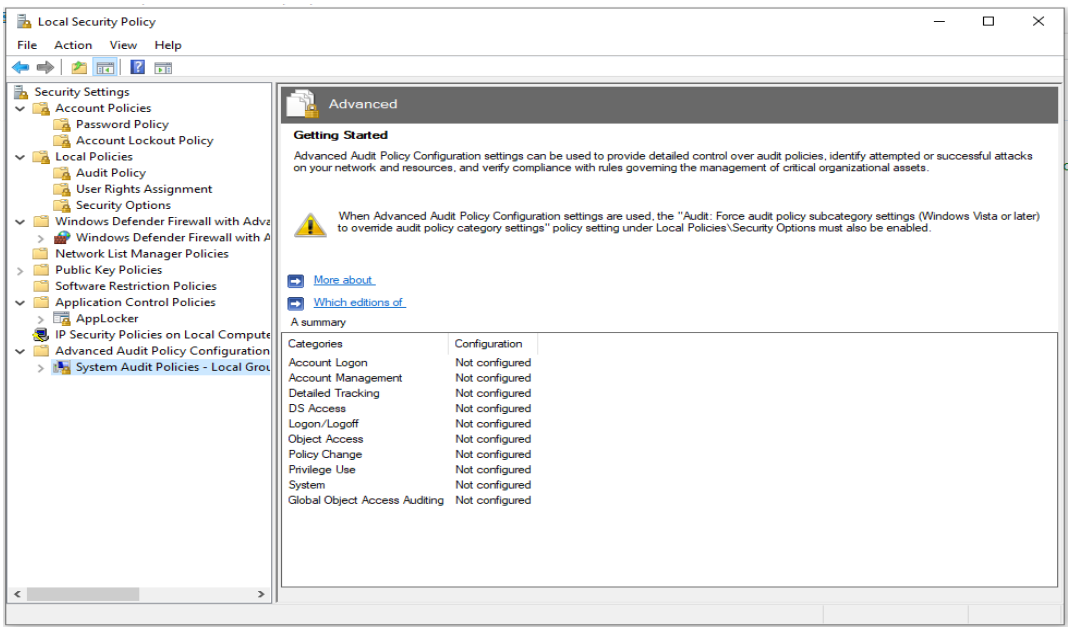
Таким чином я заборонив доступ для усіх користувачів до програми, які не мають права Адміністратора.

1.4.6 **Засіб "Конфігурації розширеної політики аудиту"**

Засіб "Конфігурації розширеної політики аудиту" (Advanced Audit Policy Configuration) в операційній системі Windows дозволяє налаштовувати докладніші аудит-політики для моніторингу подій безпеки в системі. Цей засіб надає більш гранульований контроль над аудит-функціями, ніж стандартні політики аудиту.Для доступу до "Конфігурації розширеної політики аудиту" виконую такі кроки:

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration)
3. У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).

4.Розгортаю розділ "Аудиторські політики" (Audit Policy) і переходжу до "Конфігурації розширеної політики аудиту" (Advanced Audit Policy Configuration).



Рисунок

У "Конфігурації розширеної політики аудиту" ви можете налаштовувати наступні параметри аудиту:

1. Об'єктні аудит-політики:
    - Дозволяє налаштовувати аудит певних об'єктів, таких як файли, папки, реєстри, об'єкти Active Directory і т. д.
    - Можна вказати, які події повинні бути аудитовані для кожного об'єкту, наприклад, доступ до об'єкту, зміна об'єкту, видалення об'єкту і т. д.
2. Аудиторські політики для процесів, ядра та системних служб:
    - Налаштовування аудиту подій, що стосуються процесів, ядра операційної системи і системних служб.
    - Можна включити аудит запуску та зупинки процесів, неправомірні дії ядра, зміни конфігурації системних служб і т. д.
3. Аудиторські політики для входу/виходу, об'єктів каталогів та керованих служб:
    - Налаштовування аудиту подій, пов'язаних зі входом та виходом користувачів, маніпуляціями з об'єктами каталогів (наприклад, доступ до Active Directory) та змінами керованих служб.

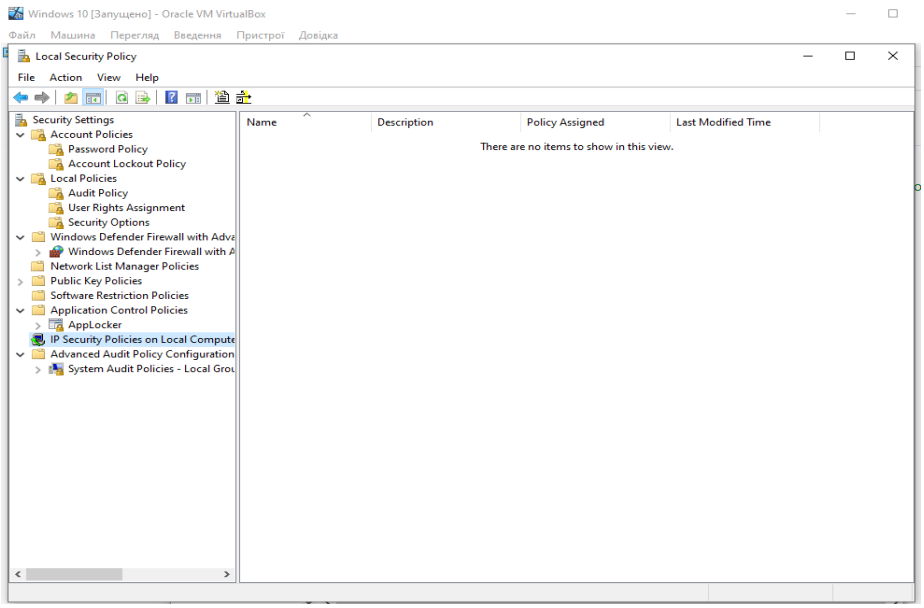
Ці політики аудиту дозволяють адміністраторам встановлювати детальніші налаштування для моніторингу подій безпеки в системі, що допомагає виявляти та реагувати на потенційні загрози та інциденти безпеки.

1.4.7 **Засіб "Політики IP-безпеки"**

Засіб "Політики IP-безпеки" (IP Security Policies) в операційній системі Windows дозволяє налаштовувати політики безпеки на рівні IP-адреси, що забезпечує контроль над комунікацією мережевих пристроїв і захищає мережеві ресурси від небажаних зовнішніх доступів.

Для доступу до "Політик IP-безпеки" виконую такі кроки:

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration)
3. У цьому розділі знаходжу та обираю "Локальна безпекова політика" (Local Security Policy).
4. Розгортаю розділ "Політики безпеки локального комп'ютера" (Local Policies) і переходжу до "Політик IP-безпеки" (IP Security Policies).



У "Політиках IP-безпеки" ви можете налаштовувати наступні параметри:

1. Загальні налаштування IP-безпеки:
    - Визначення загальних налаштувань, таких як активування або деактивування IP-безпеки, використання захищених з'єднань та інших параметрів безпеки мережі.
2. Політики IP-фільтрації:
    - Встановлення правил IP-фільтрації, що контролюють доступ до мережевих ресурсів на основі IP-адрес, портів, протоколів тощо.
    - Вказання дозволених або заборонених з'єднань для різних мережевих ресурсів із заданими умовами.
3. Правила безпеки IPSec:
    - Налаштування правил IPSec для захисту мережевого трафіку шляхом шифрування, аутентифікації і інтегритету даних.
    - Встановлення захищених тунелей для забезпечення безпеки комунікації між мережевими пристроями.
4. Управління сертифікатами:
    - Керування сертифікатами безпеки для використання в IPSec тунелях і аутентифікації.

Ці політики IP-безпеки дозволяють адміністраторам контролювати безпеку мережі на рівні IP-адреси та застосовувати захисні механізми для захисту мережевих ресурсів та комунікації в системі..

1.4.8 **Засіб "Брандмауер Windows"**

Засіб "Брандмауер Windows" (Windows Firewall) є вбудованим захисним механізмом в операційну систему Windows, який контролює вхідний та

вихідний мережевий трафік і захищає комп'ютер від небажаних підключень та зовнішніх загроз.

У "Брандмауері Windows" ви можете налаштовувати наступні параметри безпеки:

1. Профілі брандмауера:
    - Для різних типів мереж (наприклад, домашня, робоча або громадська) можна встановлювати різні правила брандмауера.
    - Кожен профіль має власні налаштування безпеки, які можна налаштовувати окремо.
2. Вхідні правила:
    - Визначення правил, які контролюють вхідний мережевий трафік до комп'ютера.
    - Можна дозволити або блокувати певні порти, протоколи або програми.
3. Вихідні правила:
    - Встановлення правил, які контролюють вихідний мережевий трафік з комп'ютера.
    - Можна дозволити або блокувати певні порти, протоколи або програми.
4. Розширені налаштування:
    - Налаштування додаткових параметрів брандмауера, таких як безпека доменних профілів, блокування відомих шкідливих програм, налаштування безпеки підключення через громадські мережі тощо.

"Брандмауер Windows" надає адміністраторам можливість контролювати мережевий трафік і захищати комп'ютер від небажаних підключень, загроз та зловмисних програм. Це допомагає підвищити безпеку системи і захистити конфіденційні дані.

Налаштування доступа до мереж окремим програмам

1. Відкриваю "Панель управління" (Control Panel).
2. Обираю "Адміністрування" (Administration)
3. У цьому розділі знаходжу та обираю "Брандмауер Windows" (Windows Firewall).

Рисунок 1.72 Вікно Брандмауера Windows

4 Натискаю Додаткові параметри, після чого відкривається вікно Windows Defender Firewall with Advanced Security

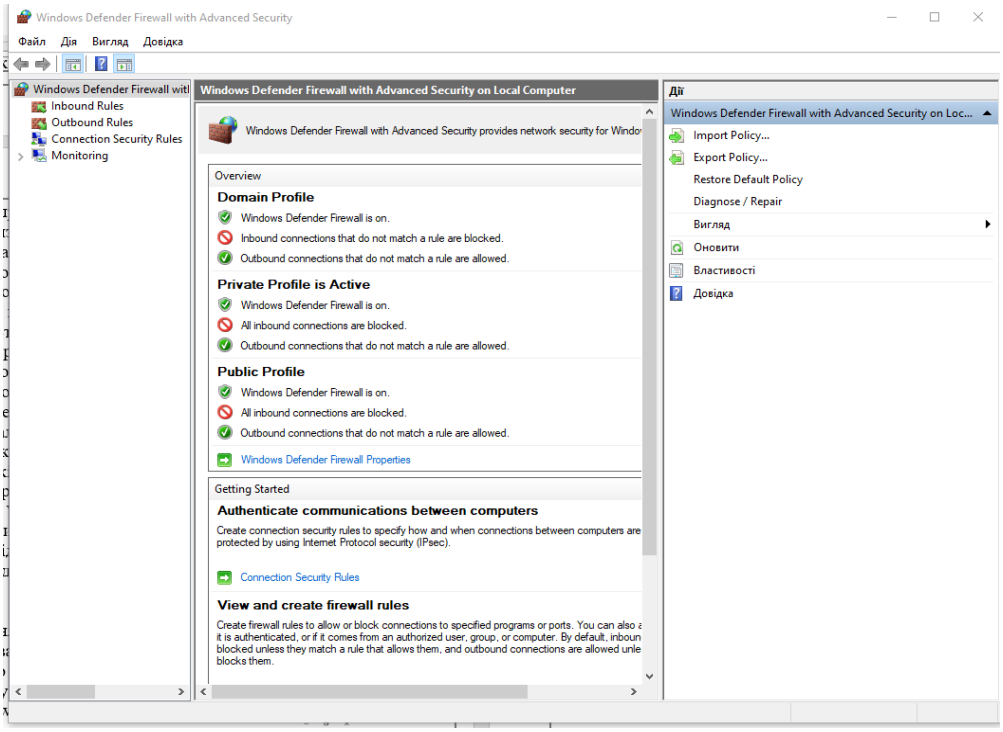


Рисунок 1.73 Windows Defender Firewall with Advanced Security

На Рис. 1.74 можна побачити вже згенеровані правила підключення інших програм

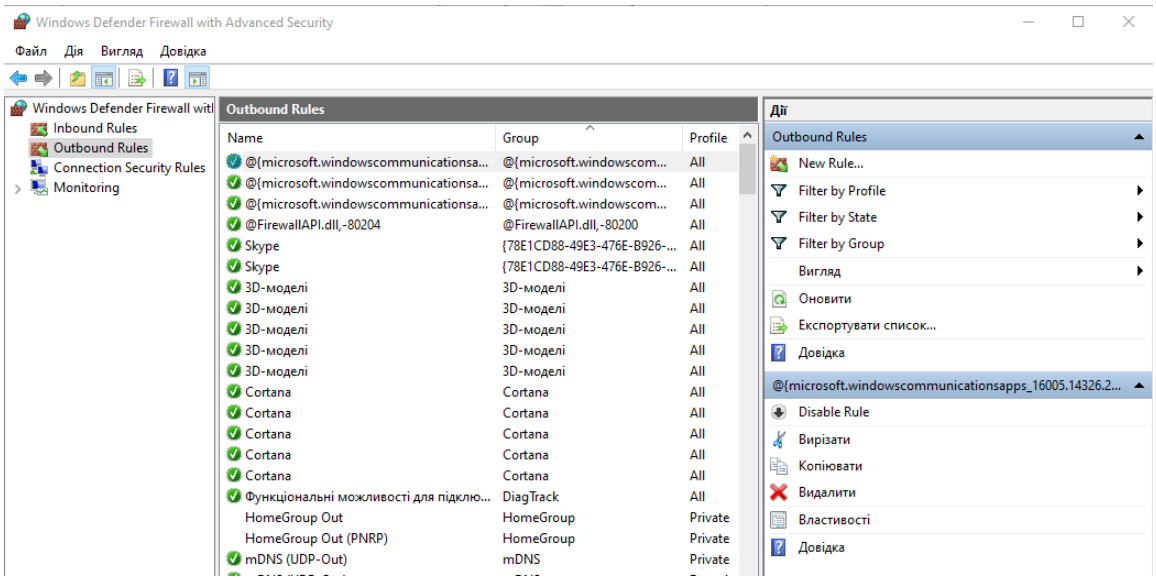


Рисунок 1.74 Список правил підключень

5 Заходжу у вкладку Outbound Rules та обираю New Rule

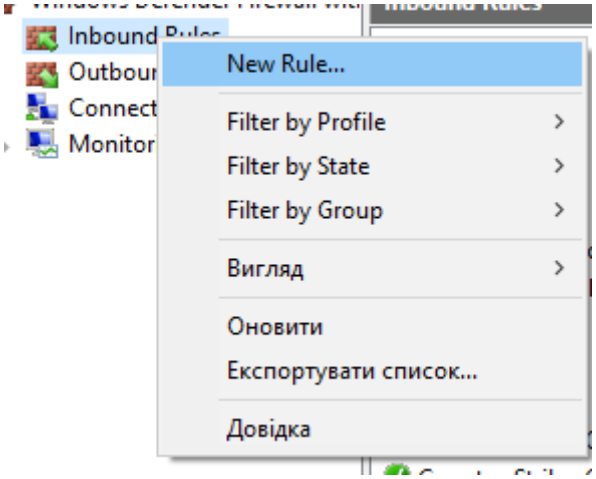


Рисунок 1.75 Контексте меню Inbound Rules

6 Ставлю прапорець на Program і натискаю Next

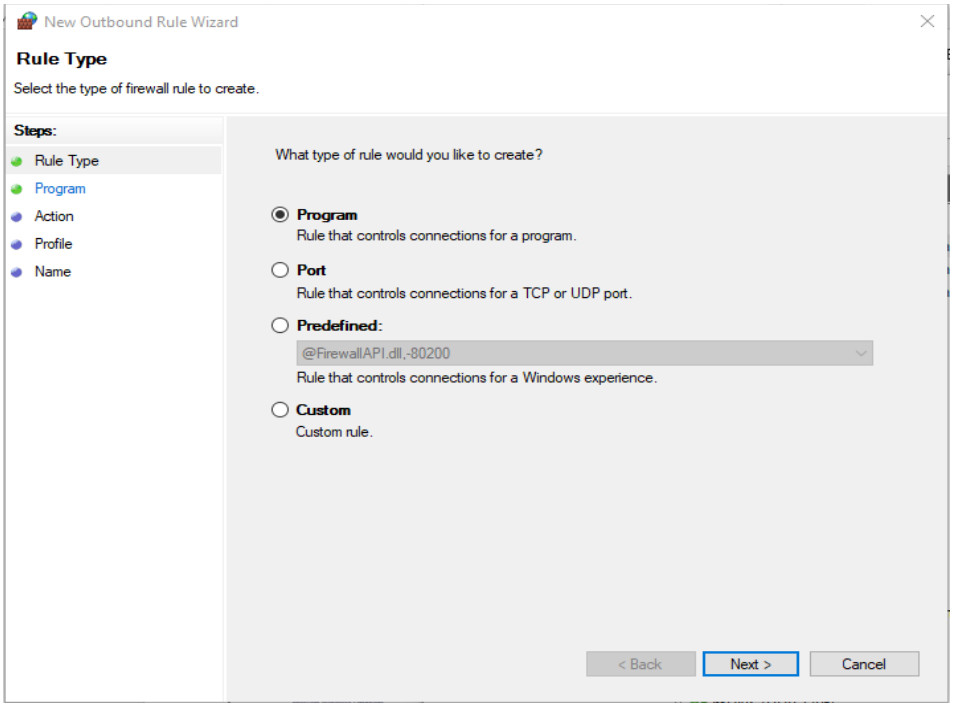


Рисунок 1.76 Тип створюйомого правила

7 Обираю This program path і Next

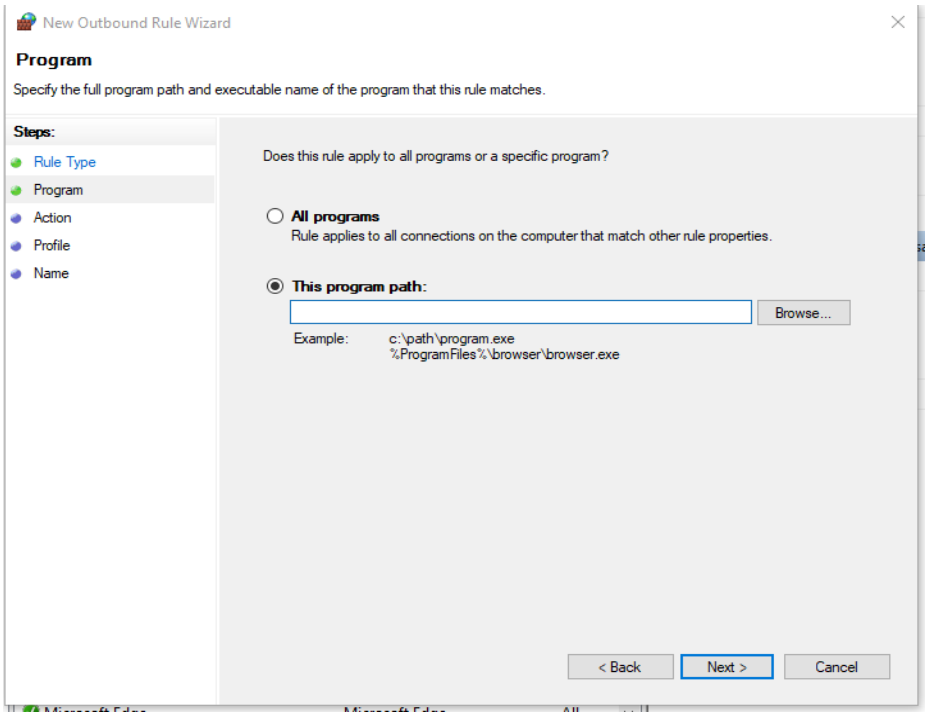
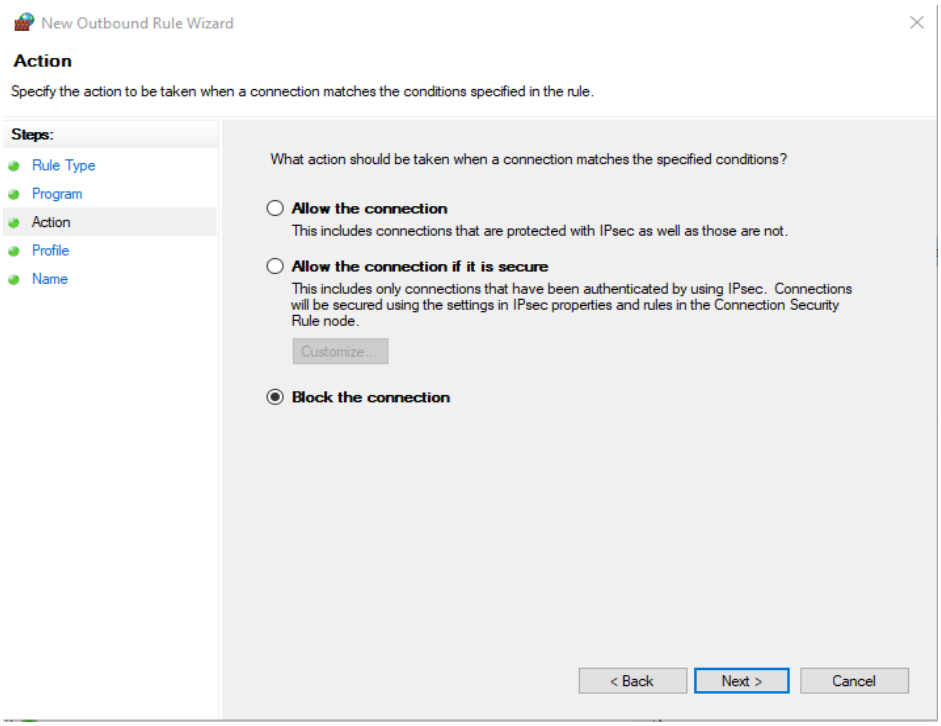


Рисунок 1.8 Вікно для обіру шляху програми

8 Задаю директорію програми C:\ProgramFiles\Google\ Chrome\ Application\ chrome.exe і натискаю Next

9 Далі обираю Block the connection і Next, в наступному вікні натискаю Finish



10 Так само створюю правило у Inbound rules

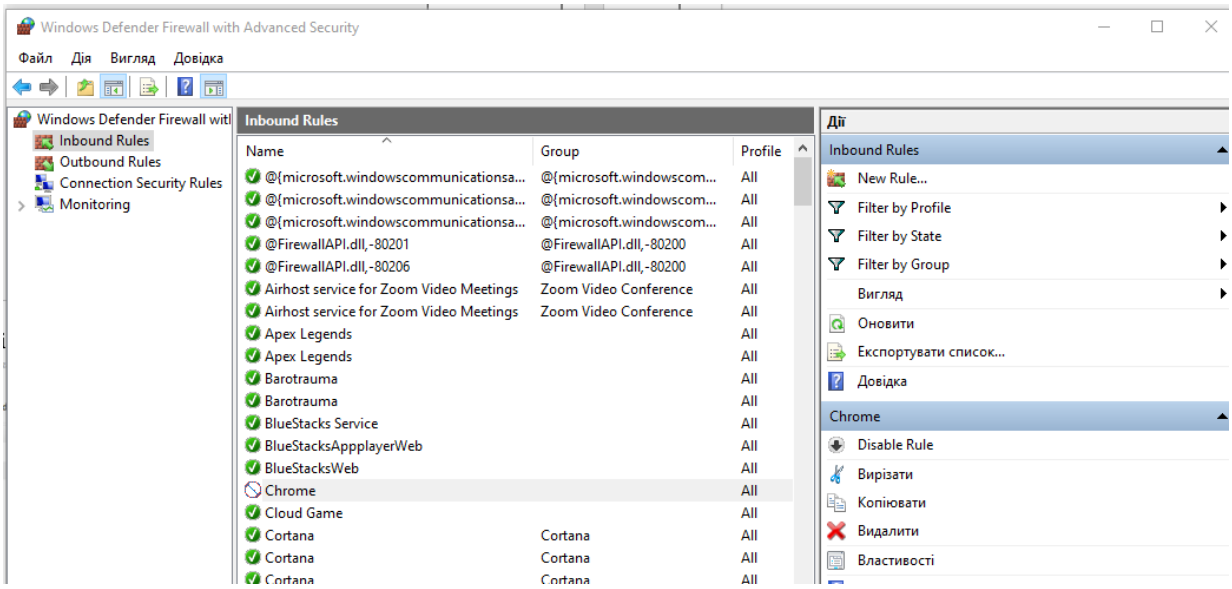
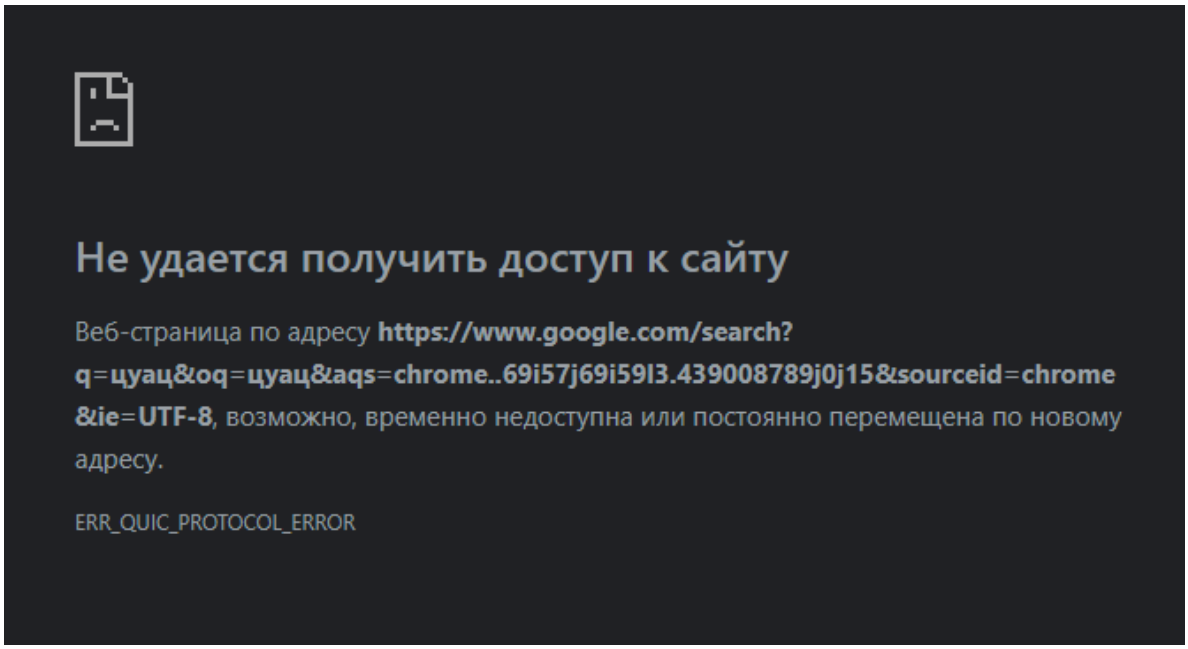


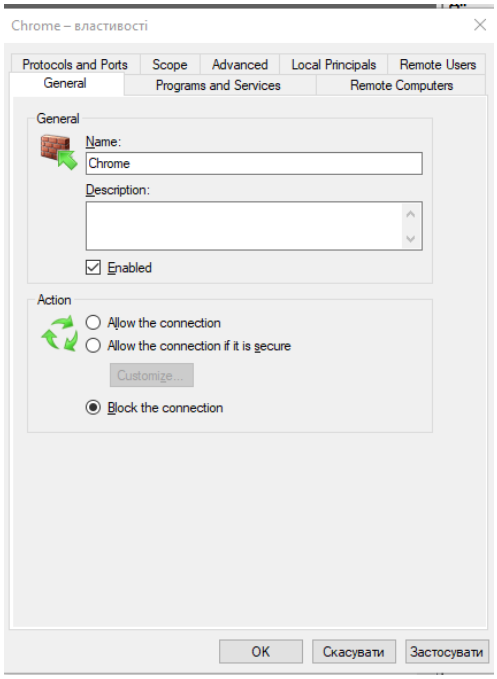
Рисунок Вкладка Inbound Rules

11 Тепер заходжу у браузер Chrome , і намагаюся зайти на сайт будь який, щоб перевірити чи є з’єднання з інтернетом.



Рисунок

12 Повертаюсь у вкладку з Outbound rules і заходжу у властивості створеного правила



13 Обираю Allow the connection і натискаю ОК

14 Роблю аналогічно для Outbound rules

15 Повертаюся до браузеру Chrome та оновляю сторінку

Рисунок 1.81 Вікно браузера

Як можна побачити , завдяки брандмауеру та його налаштуванням , можна забороняти або давати доступ до мереж системи за допомогою правил підключень.

2 ЕКОНОМІЧНА ЧАСТИНА

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи «Розробка та реалізація локальної політики безпеки комп’ютерної системи за допомогою сервісів Windows» У дипломній роботі було розглянуто локальна політика безпеки комп’ютерної системи, файлова система NTFS, аудит ресурсів і подій системи захисту, засоби для базової конфігурації політики безпеки. Усе це допомагає налаштувати систему під користувачів та захистити комп’ютерну систему від несанкціонованого доступу.

Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення.

Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців. Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Розподіл робіт по етапах і видах виконавців.

Розподіл робіт по етапах і видах виконавців.

Таблиця2.1 **Розподіл робіт по етапах і видах виконавців.**

Етап проведення НДР	**Вигляд робіт**	**Посада виконавця**
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР по розробці “Розробка та реалізація локальної політики безпеки комп’ютерної системи за допомогою сервісів Windows”	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури. 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. 3. Вибір напряму проведення досліджень 4. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник
Теоретичні і експериментальні дослідження	1. Аналіз локальної політики безпеки комп’ютерної системи. 2. Аналіз файлової системи NTFS 3. Аналіз аудиту ресурсів і подій системи захисту Windows 10 4 Дослідження засобів для базової конфігурації політики безпеки Windows 10	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів 2. Оцінка повноти вирішення поставлених завдань. 3.Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

Оцінка тривалості виконання робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Очікувана трудомісткість робіт.Таблиця 2.2

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР	4
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	4
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Розробка плану проведення досліджень для подальшої розробки.	4
5. Аналіз локальної політики безпеки комп'ютерної системи.	2
6. Огляд методів захисту від шкідливих програм	4
7. Огляд засобів для базової конфігурації політики безпеки Windows 10	4
Всього:	24

Розрахунок собівартості і ціни виконання НДР. Виходячи з особливостей створення науково – технічної продукції і її залежності від інтелектуальної праці, розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали складають 380 грн. (Папір А4)

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2023» встановлено мінімальну заробітну плату у місячному розмірі з з 1 січня 2023 року - 6700 гривень; мінімальну погодинну тарифну ставку – 40,46 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$Зден = п.т.с. * 8;$$

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня, год.

Зден дипломника = 40,46*8 =323,68 грн.

Зден керівника = 83 *8 = 664 грн.

Зден консультантів = 60*8 =480 грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 2.3

Витрати на основну заробітну плату.Таблиця 2.3

Виконавець	**Погодинна тарифна ставка, грн**	**Денна ставка, грн**	**Трудомісткість робочих днів**	**Сума основної зарплати, грн**
Дипломник	40,46	323,68	24	7 768
Керівник	83	664	1	664
Консультант по економічній частині	60	480	0,25	120
Консультант по охороні праці	60	480	0,25	120
Нормоконтроль	55	440	0,25	110
Всього (Зо)				Зо =8 782

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

Зд=10% *Зо=8 782* 0.10

Зд= 878 грн

4)До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає:

Зєсв=0,22*(Зо+Зд)=0,22*(878+8782)

Зєсв=2 125 грн.

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР. У наукових

закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

Рнакл= (Зо+Зд)*0,4=0,4*(878+8782)

Рнакл=3 864 грн.

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4

Таблиця 2.4 **Калькуляція планової собівартості**

Статті витрат	Сума, грн.
1. Матеріали	380
2. Основна заробітна плата	8 782
3. Додаткова заробітна плата	878
4. Відрахування до єдиного соціального внеску	2 125
5. Накладні витрати	3 864
Планова собівартість (Спл)	16 029

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл = 1602 грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі

Цнір = Спл + Ппл = 17 631 грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

ПДВ = 0,2*Цнір= 3 526 грн.

Звідси ціна реалізації становить:

Цр = Цнір + ПДВ= 21 157 грн.

3 ОХОРОНА ПРАЦІ

Вирішення завдань охорони праці базується на досягненнях ергономіки, наукової організації праці, технічної естетики, гігієни та фізіології праці, психофізіології. Крім того, успіх охорони праці визначається темпами впровадження передової техніки, підвищення рівня механізації і автоматизації виробничих процесів, удосконаленням технології та організації виробництв.

Безпека праці на підприємстві може бути на належному рівні тільки тоді, коли всебічно відповідає вимогам трудового законодавства, державним стандартам України, норм і правил, розроблених для збереження здоров'я працюючих. Важливе місце при цьому належить виконанню організаційних вимог з охорони праці, а також трудовій та виробничій дисципліні працюючих.

Дипломним проектом розглядається питання розробки та реалізації локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows, що передбачає працю з використанням персонального комп'ютера. Тому до розгляду в даному розділі беремо працю програміста та питання забезпечення його здорових умов праці.

1.Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

На робочому місці розробників програмного забезпечення: підвищене електромагнітне випромінювання, статична електрика, високий рівень шуму, несприятливі мікрокліматичні умови, підвищене навантаження на зір і мозок. Робота з комп'ютером - це передусім робота з фіксованою продуктивністю, розумова праця. Тому постійний вплив може призвести до професійних захворювань, таких як захворювання органів зору, опорно-рухового апарату, нервової системи та перевтоми.

2 Гігієнічні вимоги до виробничого середовища.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою

ЕОМ. В процесі роботи з комп'ютером необхідно дотримувати правильний режим праці і відпочинку.

2.1 Вимоги до приміщення

Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше 6,0 м^2, а об’єм – не менше ніж 20,0 м^3. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги. При приміщеннях мають бути обладнанні побутові приміщення для відпочинку.

Обємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПІН 3.3.2.007-98.

2.2 Освітлення

Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення, відповідно до ДБН В.2.5-28-2018. У приміщеннях доцільно, щоб вікна були орієнтовані на північ або північний захід. На вікнах повинні бути штора або жалюзі, що регулюють рівень освітленості і захищають від прямого влучення сонячних променів на робоче місце. При кольоровому оформленні виробничих і допоміжних приміщень необхідно враховувати орієнтацію їхніх вікон стосовно частин світу і використовувати гармонійне сполучення кольорів. Для стін і робочих поверхонь використовують мало насичені (основні) кольори, для невеликих помешкань або ділянок, що рідко потрапляють у поле зору працюючих, а також для створення контрастності – кольори середньої насиченості (допоміжні), для маленьких по площі

поверхонь – насичені (акценти) – як функціональне фарбування.

Стелі у всіх приміщеннях повинні бути білими. Поверхні устаткування в приміщеннях повинні бути матовими або напівматовими, для виключення випадку відблисків світла в очі працюючого, а стіни бути пофарбованими фарбами пастельних тонів.

2.3 Шум

Оптимальні показники рівня шумів у робочих приміщеннях конструкторськихбюро, кабінетах розраховувачів, програмістів визначаються за ДСТУ 2867-94. Припустимий рівень шуму при розумовій праці, що вимагає зосередженості для програміста, - 50 дБ. Для зменшення шуму й вібрації в приміщенні устаткування, апарати й прилади встановлюються на спеціальні фундаменти й прокладки, що амортизують. Якщо стіни й стелі приміщення є джерелами шумо-утворення, вони повинні бути облицьовані звуковбирним матеріалом.

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення повинні бути облицьовані звуковбирним матеріалом.

2.4 Мікроклімат

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря – ДСН 3.3.6.042 – 99 Санітарні норми мікроклімату виробничих приміщень..

Параметри мікроклімату	значення параметрі	
	Взимку	влітку
Температура, C^0	22-24	23-25
Відносна вологість, %	40-60	40-60
Швидкість руху повітря, м/с	0,1	0,1-0,2

Для підтримки в приміщеннях нормального, що відповідає гігієнічним вимогам складу повітря, видалення з нього шкідливих газів, пилу використовують вентиляцію. Механічна вентиляція (кондиціонери, вентилятори і т.д.) залежно від напрямку руху повітряних потоків, може бути витяжною, припливною і припливно-витяжною. При природній вентиляції (за допомогою вікон) повітря надходить у приміщення і видаляється з нього внаслідок різниці температур і тиску.. Механічна вентиляція забезпечується вентиляторами, що забирають повітря зовні і направляє його до будь-якого робочого місця. або устаткування, а також видаляють забруднене повітря

2.4 Вимоги до організаціїробочого місця працівника

Велике значення має раціональна конструкція та розташування елементів робочого місця, що важливо для підтримки оптимального робочого стану для працівника.

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео термінала, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

Висота робочої платформи повинна становити від 680 до 800 мм, а її ширина повинна регулюватися таким чином, щоб робоча зона була в межах досяжності. Рекомендовані розміри робочої платформи: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм Робоче сидіння повинно бути обладнане підйомно-поворотним пристроєм для регулювання висоти і кута нахилу сидіння і спинки. Регулювання кожного параметра має бути простим,

незалежним і надійно зафіксованим.Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом $+30^0$ до нормальної лінії погляду працюючого. Клавіатуру слід розташовувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого.

3 Пожежна безпека

Пожежна безпека пристрою, що проектується у даному дипломному проекті, маєзабезпечуватися відповідно до ДСТУ 8828:2019 Пожежна безпека. Загальні положення, а вибухова безпека -- у відповідності до ГОСТ 12.1.010-76 «Взрывобезопасность. Общие требования».

Пожежна безпека - це стан об'єкта, за якого виключається можливість виникнення пожежі, запобігається розвиток пожежної небезпеки з

регламентованою ймовірністю, не створюється загроза для людей та забезпечується захист матеріальних цінностей. Системи запобігання пожеж, а також протипожежного захисту у сукупності повинні виключати вплив на людей небезпечних факторів пожежі Пожежна безпека об’єкта забезпечується:

- Системою запобігання пожежі;
- Системою протипожежного захисту;
- Організаційно-технічними заходами.

Всі приміщення повинні бути забезпечені первинними засобами пожежогасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками.

У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і приступити до ліквідації пожежі.

ВИСНОВКИ

В даній роботі розроблено та впроваджено локальну політику безпеки для комп'ютерних систем, що використовують служби Windows. Метою роботи було підвищення безпекикомп'ютерних систем на рівні локальної мережі.

В ході дослідження були вивчені основні поняття та принципи безпеки комп'ютерних систем, а також існуючі служби безпеки, що надаються операційною системою Windows. Було проаналізовано поточний стан безпеки комп'ютерних систем та виявлено конкретні недоліки та потенційні загрози.

На основі цих знань та аналізу були розроблені локальні політики безпеки, що включають конфігурацію безпеки операційної системи Windows, встановлення та налаштування додаткових служб безпеки, контроль доступу до ресурсів та моніторинг подій безпеки.

Розроблені політики було впроваджено на досліджуваних комп'ютерних системах та протестовано їх ефективність. Результати тестування показали, що впровадження локальної політики безпеки значно підвищило рівень захищеності комп'ютерних систем та знизило ризик вразливості до потенційних атак.

Отримані результати свідчать про важливість розробки та впровадження локальних політик безпеки в комп'ютерних системах на базі служб Windows. Дослідження робить практичний внесок у підвищення рівня безпеки комп'ютерних систем і може бути використане як основа для подальших досліджень і розробок у цьому напрямку.

В цілому, розробка та впровадження локальних політик безпеки для комп'ютерних систем з використанням служб Windows має великий потенціал у забезпеченні безпеки та захисту інформації, що є важливим аспектом усучасному цифровому світі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Автор: СМ Захарченко — Розподілені служби безпеки Windows

2 https://support.microsoft.com/en-gb/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963

3 https://sites.google.com/site/kmposibnyk/lekcii/tema-no9

4 https://it-community.in.ua/2010/04/lokalnaya-politika-bezopasnosti-chast-4-naznachenie-prav-polzovatelej.html/

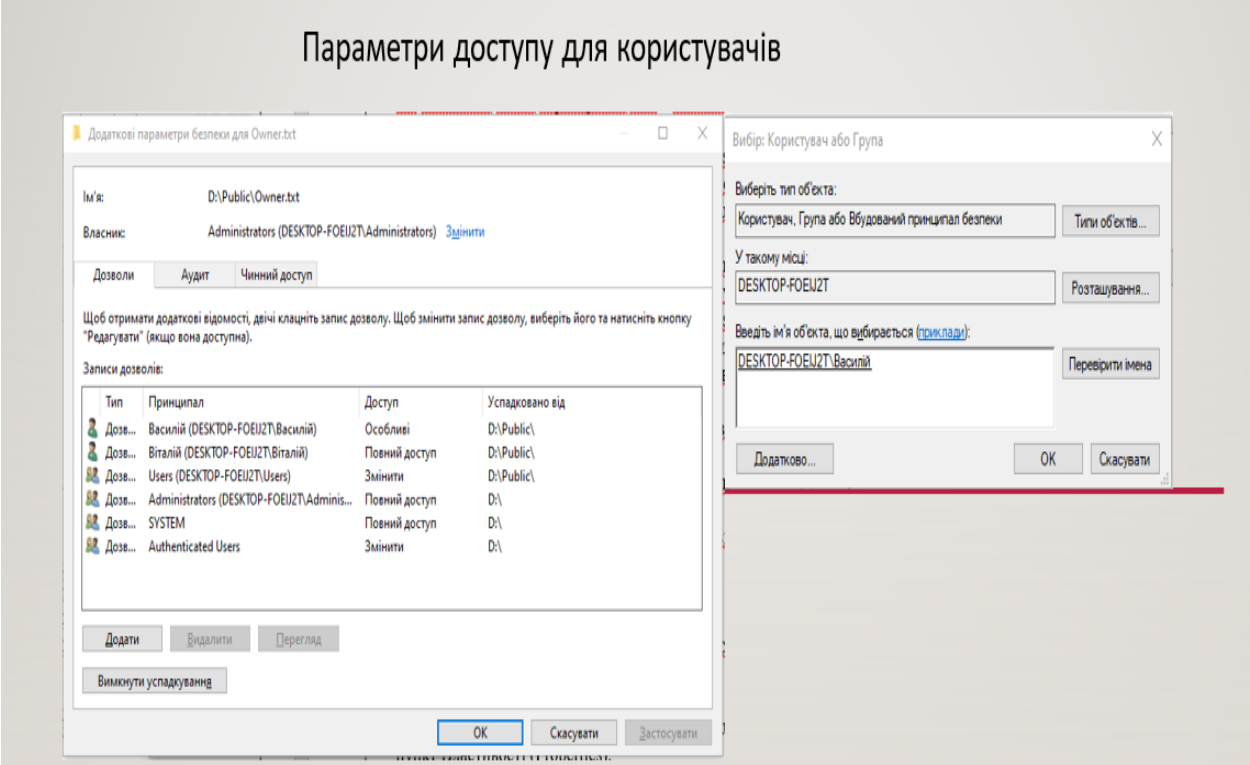
5 https://studfile.net/preview/16435895/

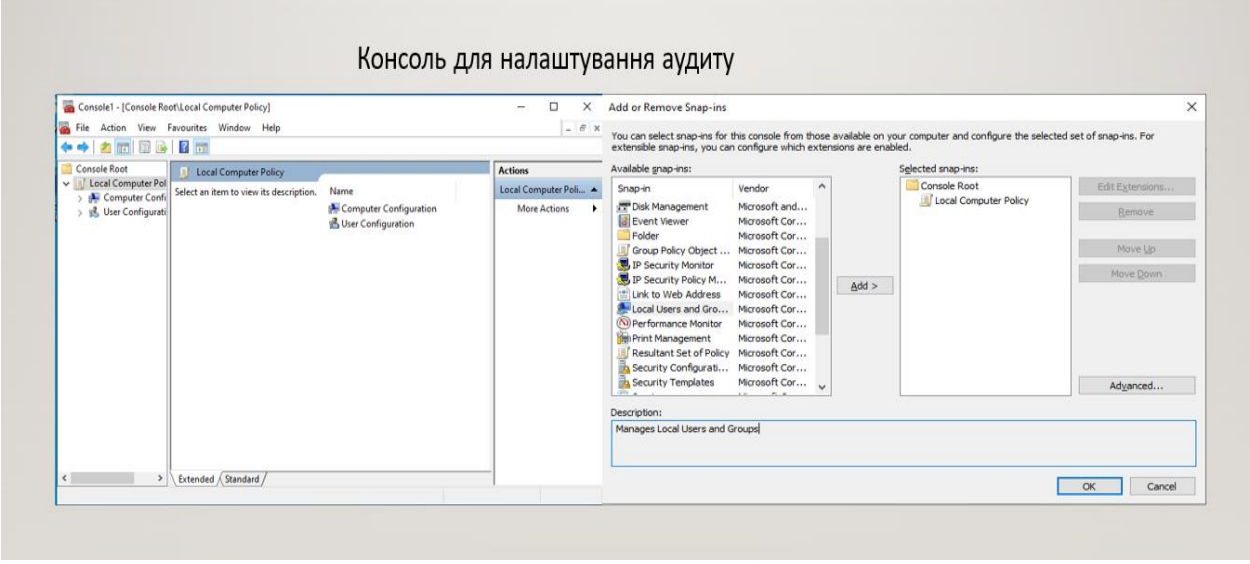
6 https://kogr.at.ua/publ/windows/os_windows/lokalnaja_politika_bezopasnosti/7-1-0-50

7 АвторБогуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П.
Основи кіберпростору, кібербезпеки та кіберзахисту 2021 рік
8 Уэнделла Одома «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640- 822»
9 Энди Ратбон. “Windows 10 для чайников.” 2018 р.
10 Самара Линн “Администрирование Microsoft Windows” 2014 р.

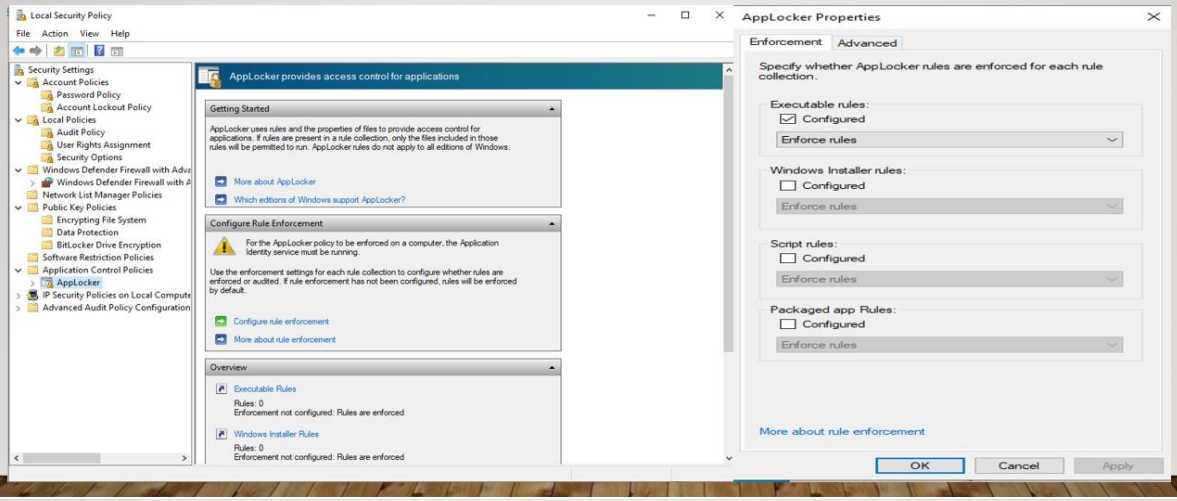
Додаток А

Слайди мультимедійної презентації

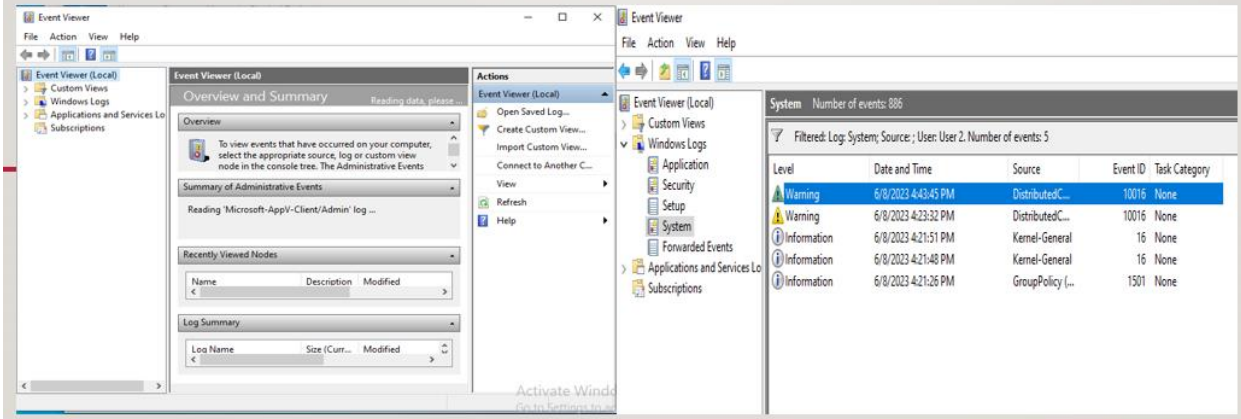




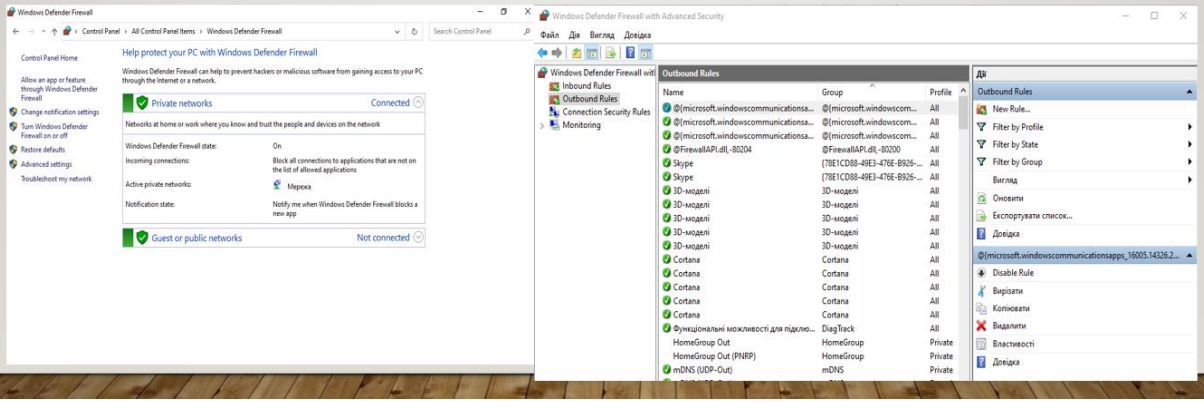
Додавання правил заборони доступу за допомогою AppLocker



Перегляд подій у системі



Створення та налаштування правил підключення мереж за допомогою Брандмауера Windows



ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти
відділення комп'ютерних систем

Биховського Марка Віталійовича

(прізвище, ім`я та по батькові)

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **Обслуговування комп'ютерних систем та мереж**

Керівник дипломного проекту (роботи) **Шевцов Юрій Сергійович**

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи)

Розробка та реалізація локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows

Обсяг розрахунково-пояснювальної записки 104 сторінок

Обсяг графічної (презентаційної) частини 10 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Дипломний проект відповідає лише частково завданню до дипломного проектування. Пояснювальна записка містить багато зайвої інформації, проте етапи проектування не відстежуються

б) характеристика виконання кожного розділу дипломного проекту (роботи)

В дипломному проекті наведені етапи налаштування локальної політики безпеки, деякі методи та засоби безпеки комп'ютерних систем. Визначені переваги сервісів Windows. Розглянуто послідовність дій налаштування сервісів безпеки Windows. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) _____

Пояснювальна записка містить багато помилок оформлення. Якість виконання невисока. Презентаційні матеріали виконані відповідають вмісту пояснювальної записки, але не несуть конструкторсько-технологічного змісту

г) перелік позитивних якостей дипломного проекту (роботи)_____

Докладно показані етапи налаштування системи безпеки Windows

д) основні недоліки дипломного проекту (роботи) _____

Робота не містить розробки чи модернізації локальної політики безпеки, проте і тема роботи зазначена невдало;

Велика кількість помилок оформлення і орфографічних помилок в тексті пояснювальної записки;

Наведено багато зайвої інформації, але аналізу не відслідковується

Оцінка розрахункової частини _____ *3(задовільно)*

Оцінка графічної частини _____ *3(задовільно)*

Загальна оцінка _____ *3(задовільно)*

Прізвище, ім'я, по батькові рецензента _____ *Василіу Євген Вікторович*

Місце роботи і посада рецензента _____ *Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки*

Підпис: _____

«16» червня 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ ДУІТЗ

НАЦІОНАЛЬНА АКАДЕМІЯ ОСВІТИ УКРАЇНИ * МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * 43997335 * ВІДДІЛ КАДРІВ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення **комп'ютерних систем**

Биховського Марка Віталійовича

(прізвище. ім'я та по батькові)

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Обслуговування комп'ютерних систем та мереж»**

Тема дипломного проекту:

Розробка та реалізація локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) **Пояснювальна записка дипломного проекту виконана якісно, у повному обсязі. В дипломному проекті здобувачем проаналізовано існуючі види засобів Windows 10 для реалізації локальної політики безпеки комп'ютерної системи. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці.**

б) самостійність роботи над проектом: **Здобувач самостійно визначався з напрямом роботи, дослухався до рекомендацій керівника дипломного проекту, пропонував рішення та своєчасно надавав результати роботи, якісно виконував основні етапи роботи за вимогою керівника.**

в) теоретична підготовка випускника (випускниці): **Теоретична підготовка випускника в цілому відповідає існуючим вимогам до фахівців відповідного рівня кваліфікації**

г) вміння розв'язувати виробничі та конструкторські питання **В процесі роботи над дипломним проектом здобувач продемонстрував уміння**

використовувати останні досягнення науки та техніки в предметній галузі, на підставі відповідної навчальної та науково-технічної літератури, пропонувати технічні рішення поставлених завдань.

Оцінка розрахункової частини 3 (задовільно)

Оцінка графічної частини 3 (задовільно)

Загальна оцінка 3 (задовільно)

Прізвище, ім`я, по батькові керівника дипломного проекту **Шевцов Юрій Сергійович**

Місце роботи і посада керівника дипломного проекту **к.т.н. доцент каф. "Електричної інженерії та електроніки" НУ «Одеська Морська академія»**

Підпис

« **12** » **червня** 20**23** р.

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015594762

Дата перевірки:
14.06.2023 09:16:01 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
14.06.2023 09:20:12 EEST

ID користувача:
100011688

Назва документа: 4ФКС-56 Биховський М.В

Кількість сторінок: 100 Кількість слів: 11475 Кількість символів: 86352 Розмір файлу: 3.01 MB ID файлу: 1015243799

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

11.4%
Схожість

Найбільша схожість: 3.29% з Інтернет-джерелом (http://um.co.ua/10/10-11/10-111593.html)

11.4% Джерела з Інтернету | 742 ..... Сторінка 102

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 28

Підозріле форматування | 41 сторінка

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Биховський Марк Віталійович
здобувач освіти гр. 4ФКС-56, та

Шевцов Юрій Сергійович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи молодшого спеціаліста на тему:

«Розробка та реалізація локальної політики безпеки комп'ютерної системи за допомогою сервісів Windows» (автор роботи – Биховський М. В., керівник роботи – Шевцов Ю.С.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Биховський М.В. /

Керівник _____ / Шевцов Ю.С./

«12» червня 2023 р.