***Модуль:* Реагування на інциденти безпеки інформації**

Практична вправа:
«Виявлення провісників та індикаторів інциденту інформаційної безпеки»

Навчальна мета заняття: навчитись виявляти провісники та індикатори інцидентів інформаційної безпеки.

Час проведення: 1 год. *Місце проведення:* комп'ютерний клас.

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веб-браузер Google Chrome.

Порядок проведення заняття

Задача 1.

1. Налаштувати ведення та забезпечення доступу до журналу подій Windows Defender Firewall.
2. Встановити Nmap Security Scanner та здійснити сканування системи, яке розглядається як підготовка до атаки.
3. Виявити провісники атаки та заповнити звіт щодо події інформаційної безпеки.

Виконання.
Через рядок пошуку відкрити Windows Defender Firewall with Advanced Security (пошуковим виразом може бути «Засоби адміністрування») (рис. 1).

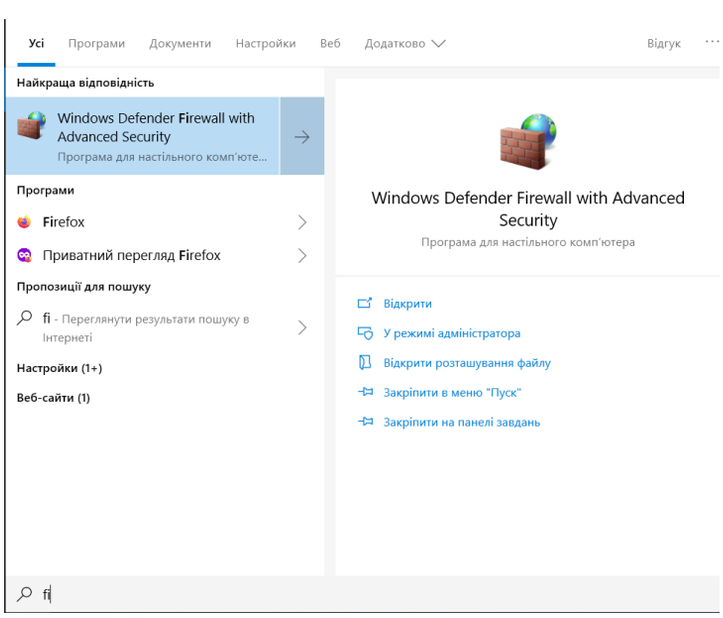

Рис. 1. Відкриття Windows Defender Firewall with Advanced Security

У Windows Defender Firewall with Advanced Security (рис. 2):

- відкрити налаштування Windows Defender Firewall Properties;
- пересвідчитись, що Firewall активований (Firewall state: on);
- для кожної вкладки Domaine Profile, Private Profile, Public Profile через опцію Logging – Customize включити записування у журнал подій про блокування мережевих пакетів (Log dropped packets: Yes) та успішне встановлення мережевого з'єднання (Log successful connections: Yes).

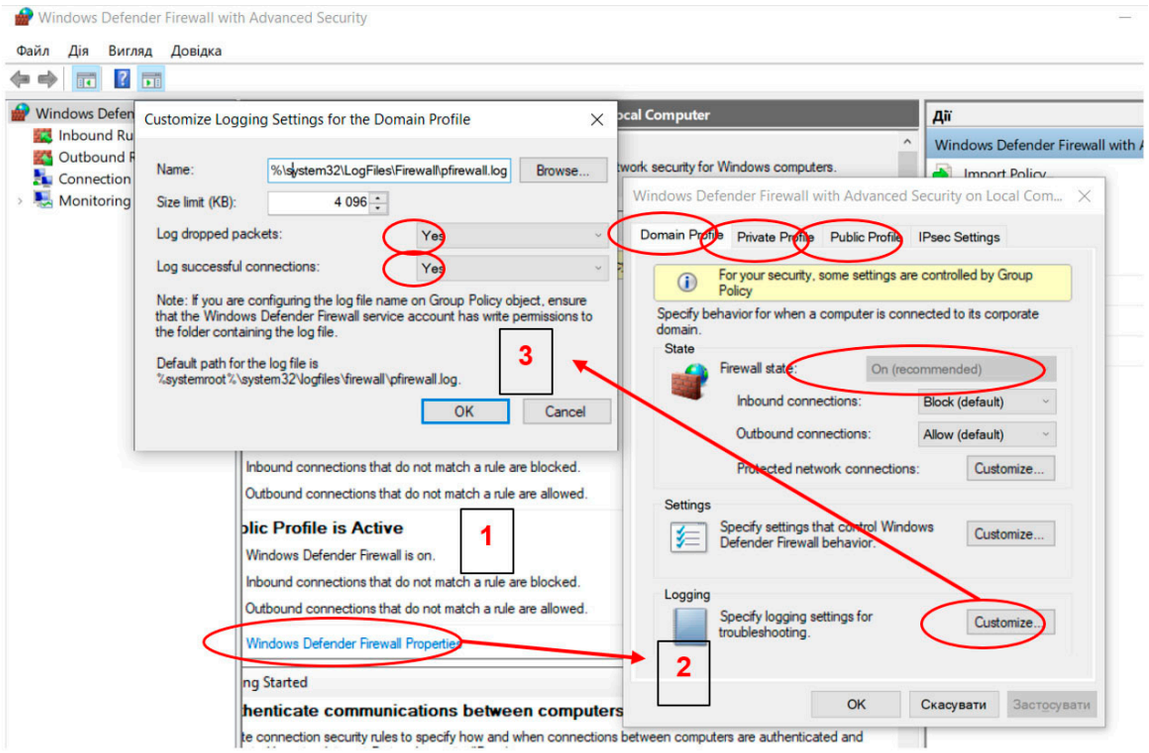

Рис. 2. Налаштування журналу подій Windows Defender Firewall

У каталозі C:\Windows\System32\LogFiles\Firewall знайти файл pfirewall.log (рис. 3).

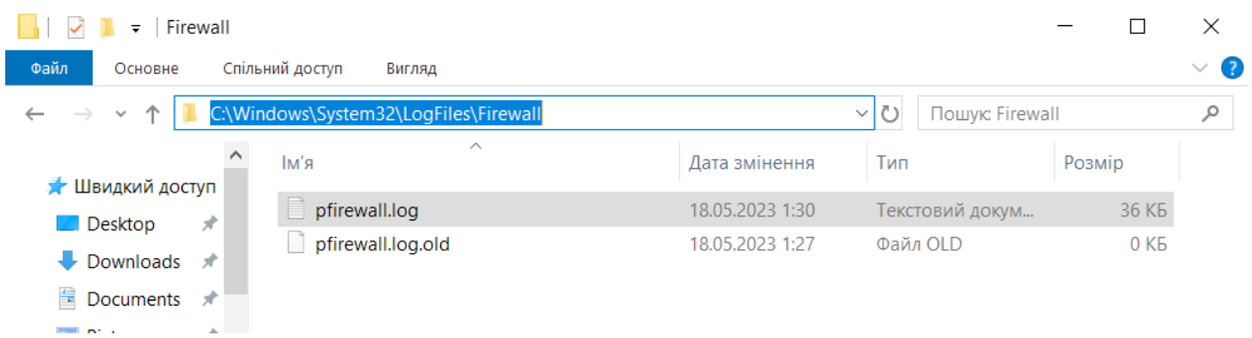

Рис. 3. Локація журналу подій pfirewall.log

Через властивості файлу pfirewall.log перейти по вкладкам Безпека – Додатково – Дозволи – Продовжити (рис. 4), а потім – Увімкнути успадкування (рис. 5).

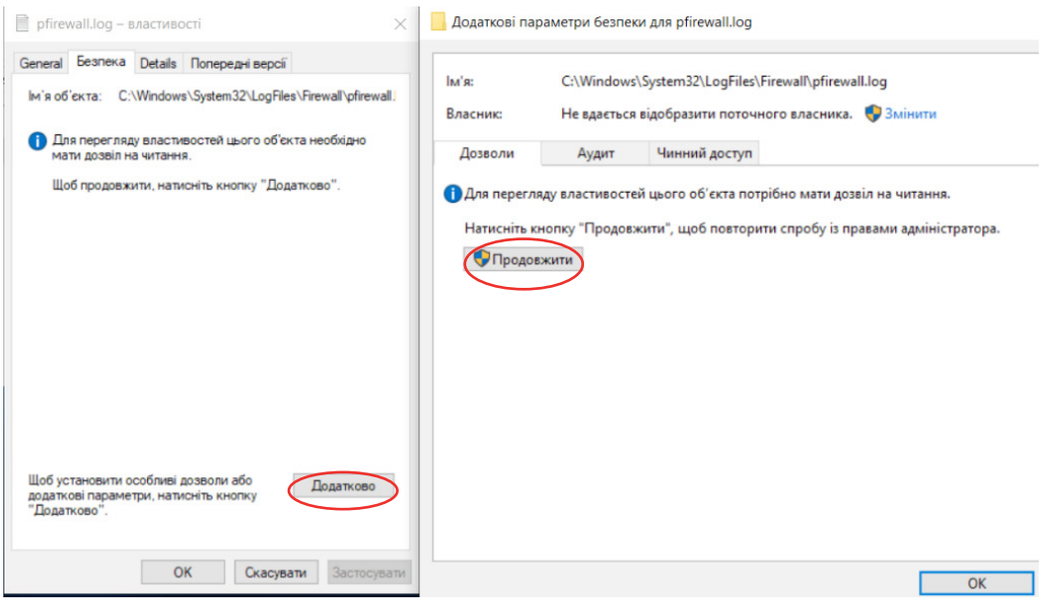

Рис. 4. Налаштування параметрів доступу до файлу pfirewall.log

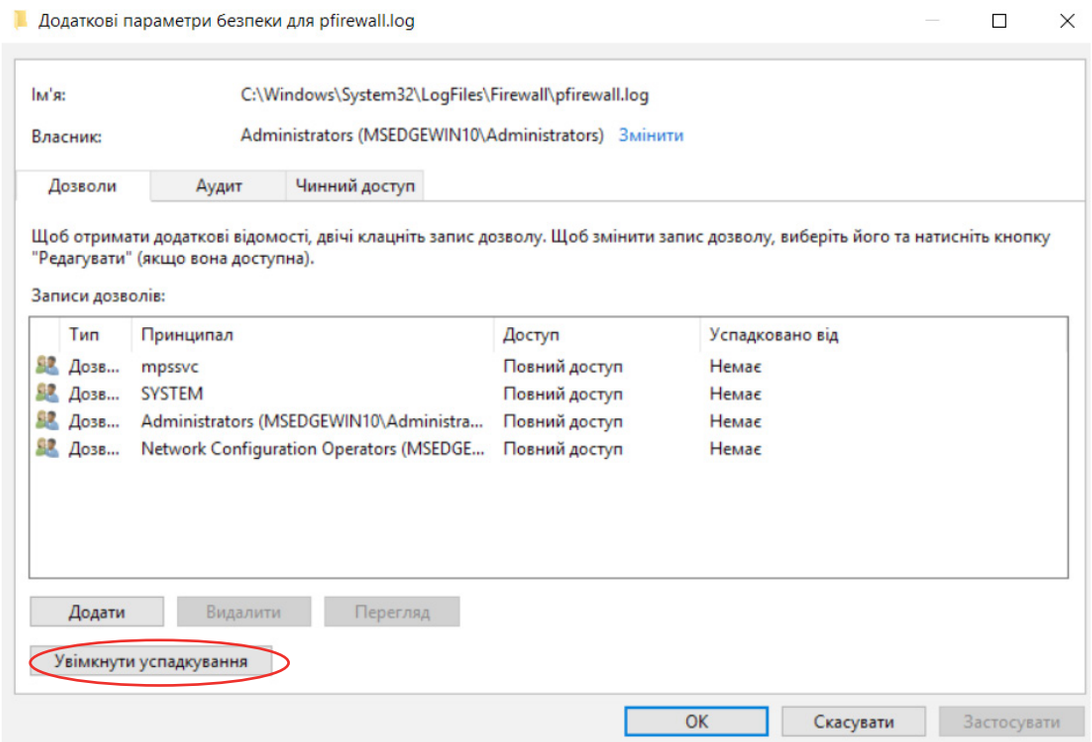

Рис. 5. Увімкнення успадкування прав доступу для файлу pfirewall.log

Переконатися, що файл журналу pfirewall.log доступний для читання, відкривши його текстовим редактором (рис. 6).

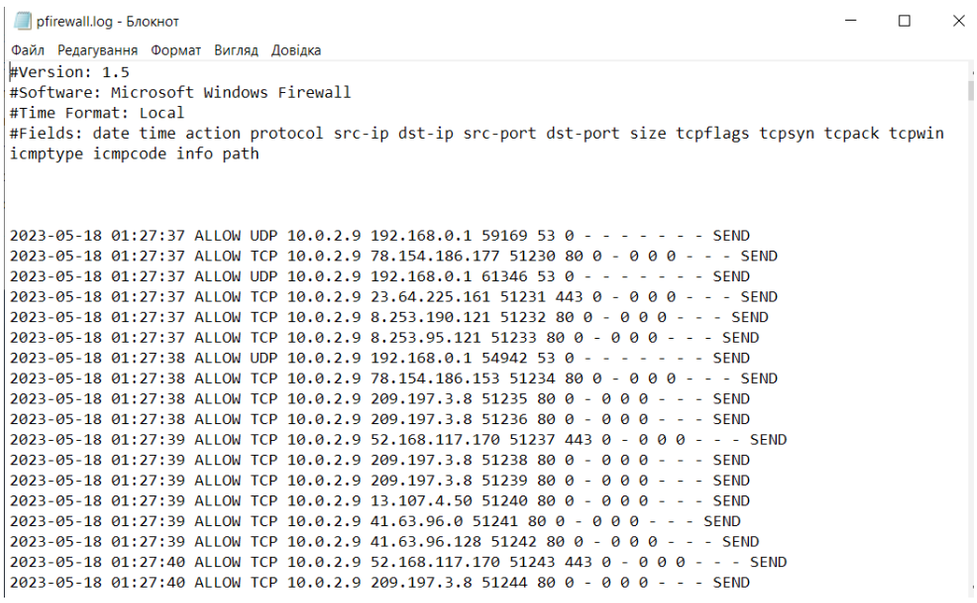

Рис. 6. Зміст журналу аудиту Microsoft Windows Firewall

У журналі аудиту Microsoft Windows Firewall (рис. 6) зазначені: дата і час, дозвіл на встановлення з'єднання (ALLOW), протокол з'єднання (UDP, TCP), IP адреси з'єднання (src-ip, dst-ip), порти з'єднання (src-port, dst-port), інше. Завантажити та встановити Nmap Security Scanner в ОС Windows (https://nmap.org/download#windows) (рис. 7).

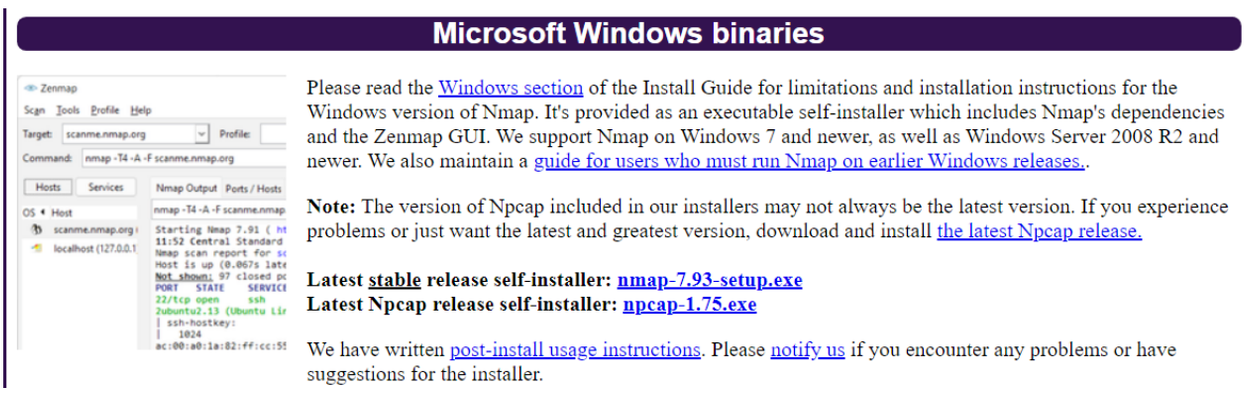

Рис. 7. Сторінка завантаження Nmap Security Scanner для ОС Windows

Відкрити сканер через ярлик «Nmap – Zenmap GUI», у полі Target вписати loopback IP адрес своєї системи: 127.0.0.1 та у режимі Quick scan plus запустити сканування (рис. 8). Сканування є підготовчим етапом перед атакою на систему, при якому здійснюється послідовний перебір портів підключення до цільової системи.

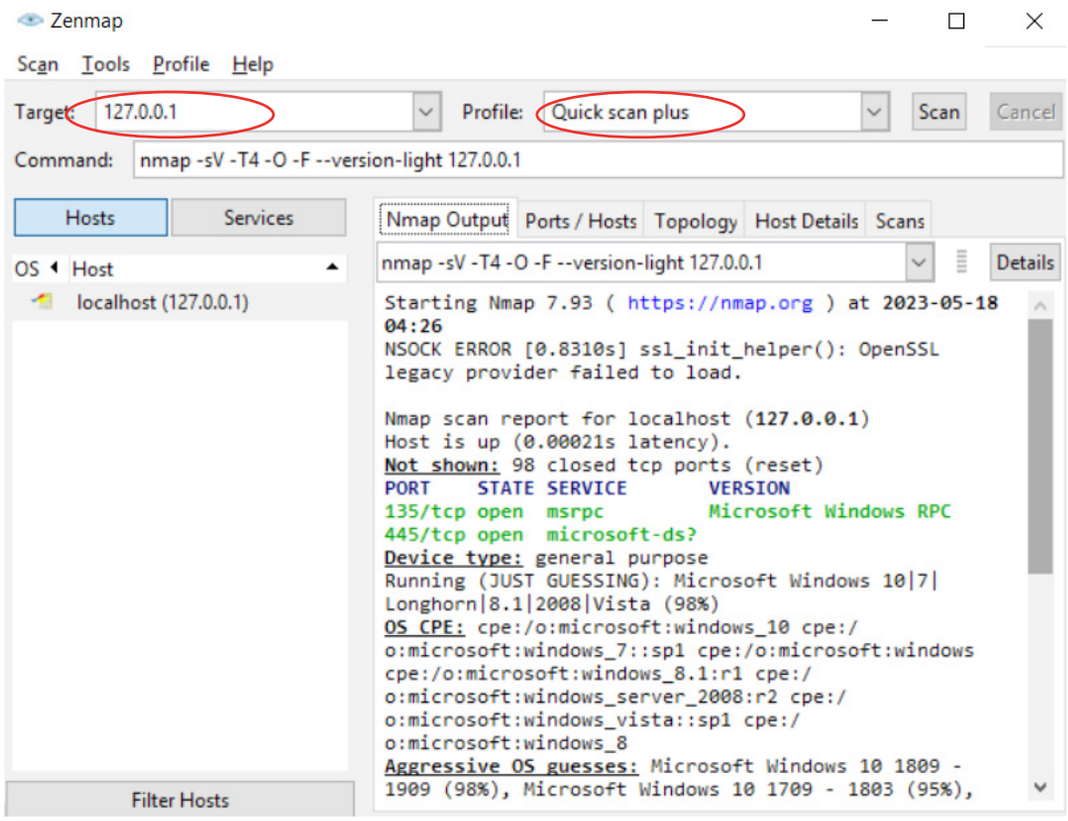

Рис. 8. Запуск сканування своєї системи

Відкрити файл журналу аудиту pfirewall.log та знайти записи, які свідчать про сканування портів системи і є провісниками майбутньої атаки на систему (рис. 9). Основною ознакою сканування є наявність великою кількості одночасних підключень з одного IP адреса до різних портів системи.

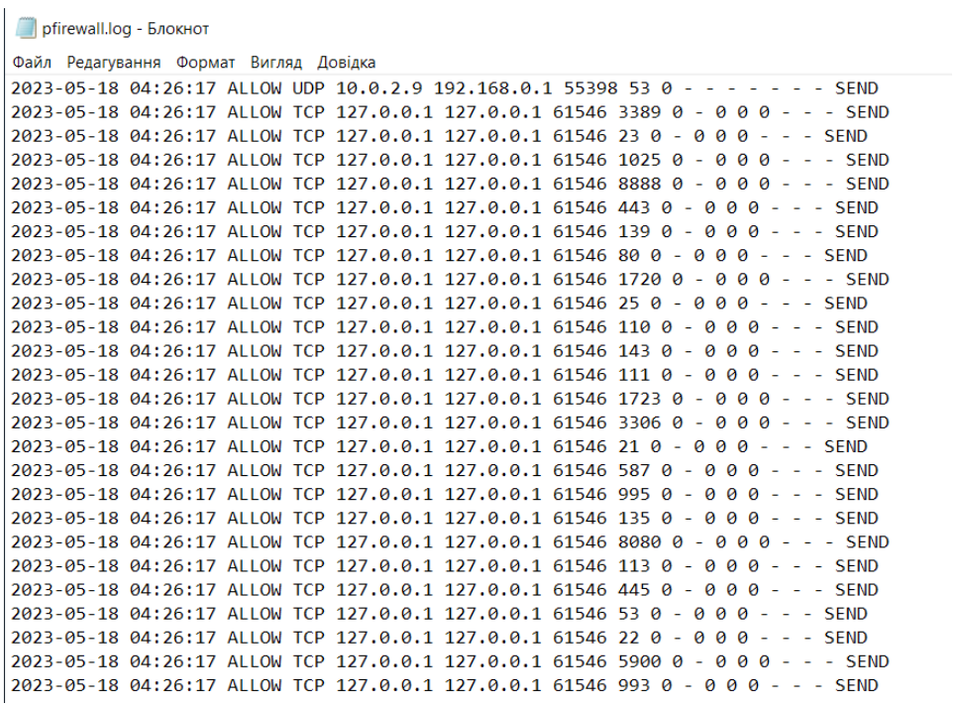

Рис. 9. Записи журналу аудиту pfirewall.log, які свідчать про сканування портів системи

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
1. Дата події	3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)
2. Номер події (надається фахівцем ISIRT)	
4. РЕКВІЗИТИ ОСОБИ, ЯКА ЗВІТУЄ	
4.1. Ім'я та прізвище	4.2. Адреса
4.3. Організація	4.4. Відділ
4.5. Телефон	4.6. E-mail
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
5.1. Опис події: • Що сталося • Яким чином сталося • Чому так сталося • Які компоненти/активи піддались впливу • Оцінка впливу на діяльність організації • Будь-які виявлені вразливості	
6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
6.1. Дата та час події	
6.2. Дата та час виявлення події	
6.3. Дата та час повідомлення про подію	
6.4. Чи відповідь на цю подію усунула небезпеку?	ТАК ☐ НІ ☐ (позначте відповідне)
6.5. Якщо так. вкажіть, скільки часу тривала подія (у днях/годинах/ хвилинах)	

Задача 2.

1. Налаштувати аудит входу користувача в систему.
2. Ввести кілька разів неправильний пароль при вході до ОС Windows.
3. Виявити індикатори інциденту інформаційної безпеки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Налаштування групової політики (Edit group policy) (рис. 10).

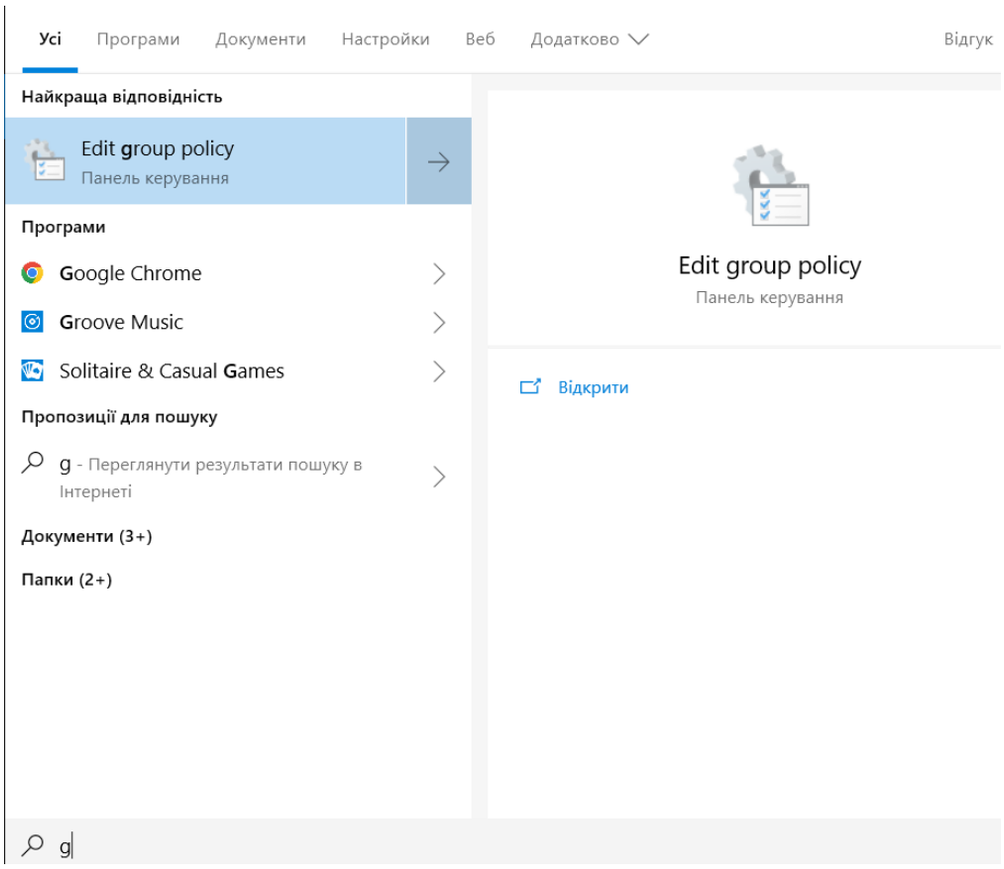

Рис. 10. Відкриття Налаштування групової політики (Edit group policy)

У розділі Конфігурація комп'ютера – Налаштування Windows – Security Settings – Advanced Audit Policy Configuration – «System Audit Policies – Local Group Policy Object» – Account Logon кликнути на параметр Audit Credential Validation та налаштувати аудит вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему (рис. 11).

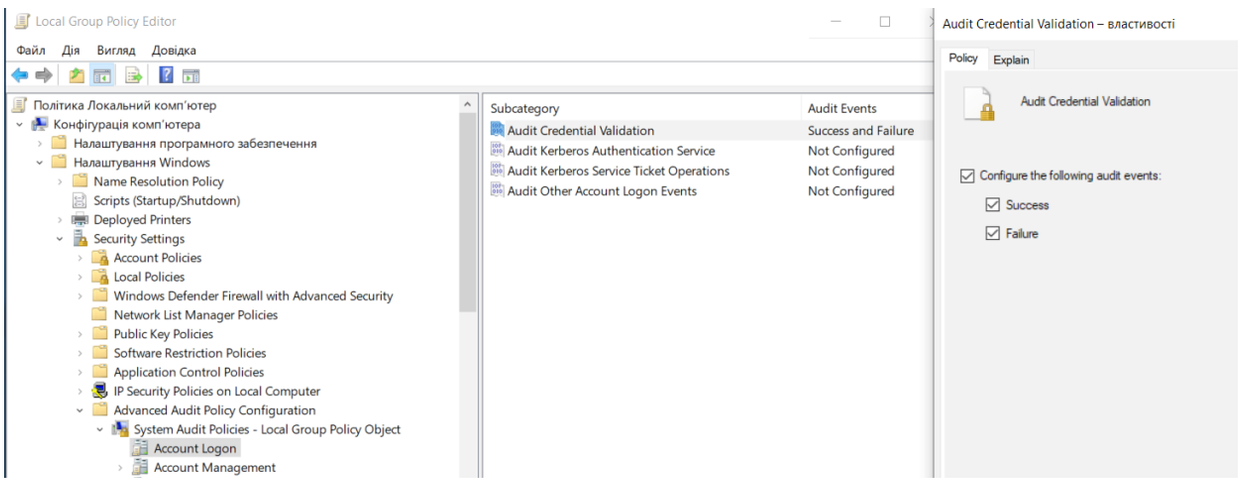

Рис. 11. Налаштування аудиту вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему

Після кількох спроб введення неправильного паролю (рис. 12) через рядок пошуку відкрити Переглядач подій (Event Viewer) – Windows Log – Security та знайти невдалі спроби вводу паролю (рис. 13).

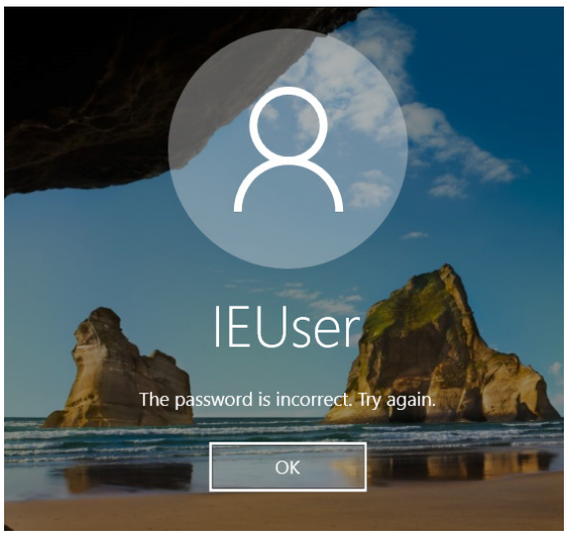

Рис. 12. Результат введення неправильного паролю

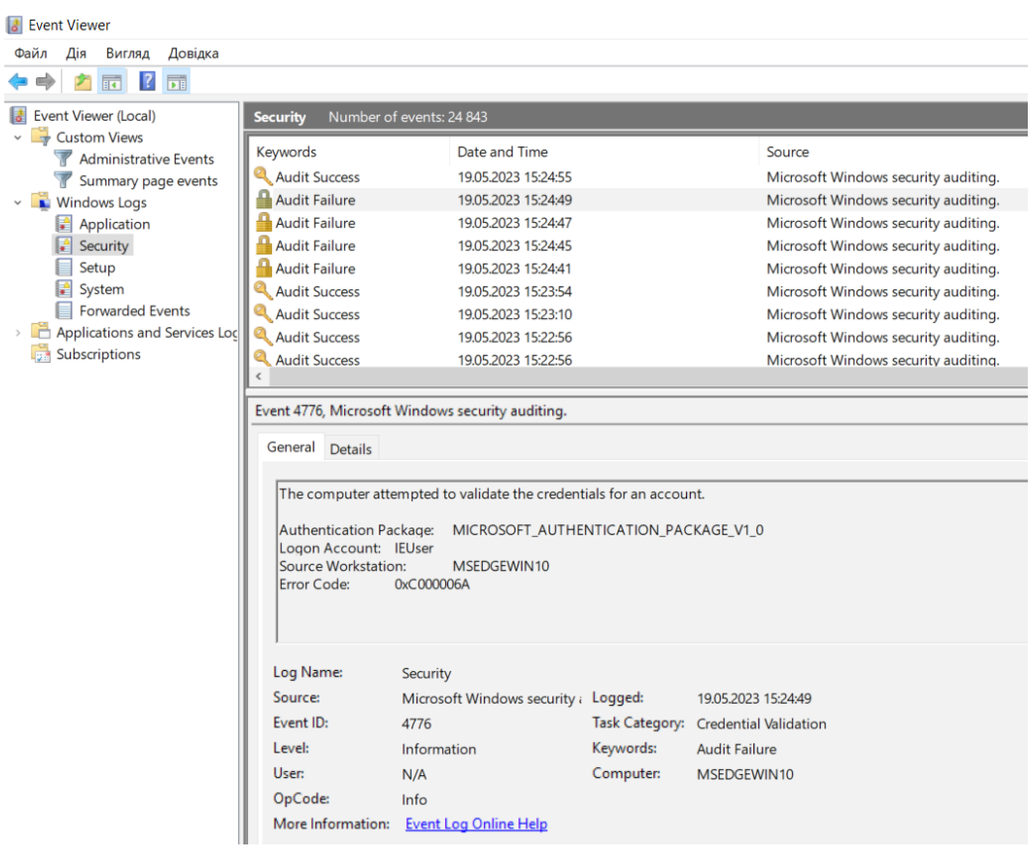

Рис. 13. Записи журналу подій про невдалі спроби входу у систему

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).