Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Використання механізмів серверних операційних систем щодо пошуку інсайдерів у корпоративних мережах
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-18-1
Лісова В.П.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського Добринін І.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентці Лісовій Валерії Павлівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Використання механізмів серверних операційних систем щодо пошуку інсайдерів у корпоративних мережах затверджена наказом по університету від «17» березня 2020 р. №465 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020 р.
3. Вихідні дані до роботи: перелік типових загроз корпоративним мережам; призначення та завдання, що вирішуються службою активного каталогу Active Directory Domain Service; розподіл випадкових і навмисних витоків інформації.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз існуючих каналів витоку інформації і аналіз частки розкриття даних через дії інсайдерів
2) Аналіз підходів щодо виявлення прихованих мереж .
3) Пропозиції щодо використання можливостей групових політик для протидії інсайдерам
4) Пропозиції щодо використання можливостей вбудованого в Windows Server аудиту для пошуку інсайдерів у корпоративних мережах

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Добринін Ігор Станіславович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.02.2020	Виконано
2	Збір матеріалів для дослідження	15.03.2020	Виконано
3	Розробка 1 розділу	25.03.2020	Виконано
4	Розробка 2 розділу	01.04.2020	Виконано
5	Розробка 3 розділу	12.04.2020	Виконано
6	Розробка 4 розділу	01.05.2020	Виконано
7	Оформлення атестаційної роботи	10.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студентка _____ Лісова В.П.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Добринін І.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 с., 36 рис., 1 табл., 2 додатки, 10 джерел.

ІНСАЙДЕР, ВИТІК ДАНИХ, ПРИХОВАНІ МЕРЕЖІ, ОПЕРАЦІЙНА СИСТЕМА, ACTIVE DIRECTORY, ГРУПОВІ ПОЛІТИКИ, РЕЄСТР, АУДИТ.

Об’єкт дослідження – система менеджменту інформаційної безпеки.

Предмет дослідження – методи й засоби пошуку інсайдерів у корпоративних мережах.

Мета роботи – аналіз способів пошуку інсайдерів у корпоративних мережах за допомогою використання механізмів серверних операційних систем, підбір найбільш ефективного механізму захисту від інсайдерських атак.

Інсайдери все частіше виявляються винними в витоках секретних відомостей, крадіжці інтелектуальної власності, фінансовому шахрайстві та саботажі IT-інфраструктури.

У роботі виконаний аналіз можливостей серверних операційних систем щодо пошуку інсайдерів у корпоративних мережах. Розроблений механізм ідентифікації інсайдера на основі вбудованих засобів операційної системи Windows Server з розгорнутими ролями Active Directory.

ABSTRACT

The report contains: 69 p., 36 fig., 1 table, 2 application, 10 sources.

INSIDER, DATA LEAK, HIDDEN NETWORKS, OPERATING SYSTEM, ACTIVE DIRECTORY, GROUP POLICIES, REGISTER, AUDIT

Object of research – information security management system.

The subject of research is methods and means of finding insiders in corporate networks through the use of mechanisms of server operating systems.

An aim of work is an analysis of ways of finding insiders in corporate networks, selection of the most effective mechanism for protection against insider attacks.

Insiders are increasingly found guilty of leaking classified information, intellectual property theft, financial fraud and sabotage of IT infrastructure.

The paper analyzes the capabilities of server operating systems to search for insiders in corporate networks. An insider identification mechanism based on the built-in tools of the Windows Server operating system with deployed Active Directory roles has been developed.

ЗМІСТ

Перелік скорочень, умовних позначень, символів, одиниць і термінів…..... 8
Вступ..... 9
1 Аналіз існуючих каналів витоку інформації і аналіз частки розкриття даних через дії інсайдерів..... 11
1.1 Джерела витоку конфіденційної інформації..... 11
1.2 Канали витоку конфіденційної інформації..... 14
1.3 Превентивні міри запобігання витоків інформації через дії інсайдерів..... 15
1.4 Пропозиції щодо організації структури корпоративної мережі, в котрій можна буде виявити інсайдера..... 17
2 Аналіз підходів щодо виявлення прихованих мереж..... 21
2.1 Використання спеціального програмного забезпечення для виявлення прихованих мереж..... 22
2.2 Використання штатних засобів Active Directory для виявлення прихованих мереж..... 27
3 Пропозиції щодо використання можливостей групових політик для протидії інсайдерам..... 37
3.1 Налаштування політик облікових записів..... 40
3.2 Налаштування політик призначення прав користувачів..... 42
4 Пропозиції щодо використання можливостей вбудованого в Windows Server аудиту для пошуку інсайдерів у корпоративних мережах..... 46
4.1 Робота з журнальними файлами..... 48
4.2 Налаштування локальних політик аудиту..... 51
4.3 Налаштування розгорнутих політик аудиту..... 55
4.4 Підсилення механізмів виявлення інсайдерів у корпоративній мережі за допомогою використання Advanced Thread Analytics…… 62
Висновки..... 67
Перелік джерел посилання..... 68

Додаток А Варіант написання скрипта для аудиту комп'ютерів в мережі з установленими ролями Active Directory Domain Service….. 70

Додаток Б Варіант скрипта для сбору інформації стосовно USB-пристроїв на ком'ютерах в мережі з установленими ролями Active Directory Domain Service……..... 71

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ОС – операційна система
AD – Active Directory
AD DS – Active Directory Domain Service
ATA – Advanced Thread Analytics
DHCP – Dynamic Host Configuration Protocol
DLP – Digital Light Processing
DNS – Domain Name System
GPMC – Group Policy Management
GPO – Group Policy Object
GUID – Globally Unique Identifier
IPC – Information Protection and Control
LDAP – Lightweight Directory Access Protocol
SSO – Single Sign On
USB – Universal Serial Bus
VID – Vendor Identifier
WinRM – Windows Remote Management

ВСТУП

Витік конфіденційних даних – це актуальна проблема для будь-якої сучасної компанії, оскільки дана подія несе за собою ряд наслідків, котрі впливають, як на фінансовий стан організації, так і на її імідж та довіру в суспільстві.

Інциденти інформаційної безпеки можуть виникати не тільки через атаки зовнішніх зловмисників, а й через вину внутрішніх співробітників компанії. Останній варіант пов’язаний з виникненням терміну інсайдер. Це може бути штатний працівник компанії, свідомі чи ненавмисні дії котрого провокують розкриття конфіденційних даних.

Метою роботи є аналіз способів пошуку інсайдерів у корпоративних мережах з контролерами домену із роллю Active Directory Domain Services за допомогою використання механізмів серверних операційних систем, підбір найбільш ефективного механізму захисту від інсайдерських атак.

Для вирішення поставленої задачі, в першому розділі атестаційної роботи проведено аналіз типових каналів витоку інформації. Доведена актуальність витоків інформації через вину інсайдера і встановлено канал, через який відбувається найбільше витоків – корпоративна мережа.

У другому розділі розглядаються причини виникнення прихованих мереж, способи їх виявлення і способи контролю інформації, що може функціонувати у цих мережах.

У третьому розділі розглянуті можливості вбудованих в Active Directory групових політик щодо мінімізації витоків конфіденційних даних через деструктивні дії інсайдерів у корпоративній мережі.

Четвертий розділ присвячений розробці механізму пошуку інсайдерів у корпоративній мережі. Розглянуті можливості аудиту подій і здійснено його налаштування. Створене централізоване сховище подій інформаційної безпеки, проаналізувавши котре можна виявити співробітника компанії, умисні дії котрого несуть загрозу для інформаційної безпеки компанії.

У Додатках А і Б наведений код двох скриптів, що використовувалися для автоматизації пошуку прихованих мереж і, відповідно, виявлення інсайдеру, дії котрого спричинили виникнення мережі.

Окремі результати роботи доповідались на XLIII Міжнародній науково-практичній інтернет-конференції «Сучасні виклики та проблеми науки» [1 – 3], на Всеукраїнської науково-практичній конференції здобувачів вищої освіти й молодих учених [4], а також на XXII Міжнародному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті» [5].

1 АНАЛІЗ ІСНУЮЧИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ І АНАЛІЗ ЧАСТКИ РОКЗРИТТЯ ДАНИХ ЧЕРЕЗ ДІЇ ІНСАЙДЕРІВ

1.1 Джерела витоку конфіденційної інформації

Робочий процес будь-якої компанії в тій чи іншій мірі пов’язаний з обробкою даних. Саме вони є одними з найважливіших та найуразливіших ресурсів організації. Розкриття інформації з обмеженим доступом може не тільки зіпсувати імідж компанії, а й завдати ризику її робочим процесам.

Останнім часом прослідковується тенденція збільшення кількості інформаційних атак. Це призводить до зростання попиту на впровадження сучасних засобів захисту – таких як, наприклад, використання надійних алгоритмів шифрування, міжмережевих екранів, систем автентифікації та систем виявлення вторгнення. Однак всі ці міри не можуть гарантувати повну відсутність вірогідності витоку конфіденційної інформації, оскільки найвразливішим місцем у системі безпеки організації залишається людський фактор.

Статистика свідчить, що значну кількість випадків розкриття даних можуть спровокувати самі співробітники компанії. Це підтверджує аналітичний звіт компанії InfoWatch [6], що був опублікований у 2019 році.

Згідно з інформацією поданій у ньому, у першій половині 2019 року внаслідок деструктивних дій штатних працівників компанії відбулося 55% випадків витоку конфіденційних даних. Це демонструє рис. 1.1 [6].

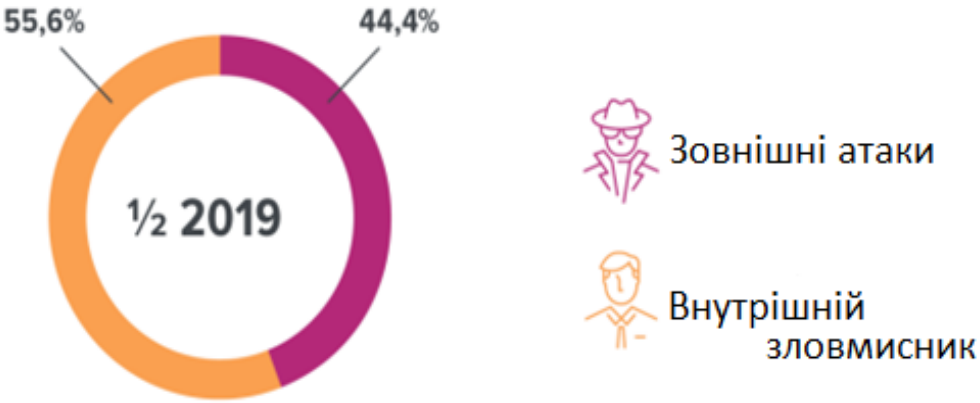

Рисунок 1.1 – Розподіл витоків інформації за вектором впливу

Також відомо, що за перше півріччя 2019 року кількість даних, скомпрометованих внаслідок дій співробітників компанії становить 4,5 млрд записів. В той час, як наслідок дій зовнішніх зловмисників – 4 млрд. Тобто проблема інсайдерських атак неабияк як актуальна, оскільки вона досягла того ж рівня, що й проблема зовнішніх спроб розкриття даних [6].

Варто відмітити, що "внутрішні" канали витоку даних можуть спричинити значно більшу кількість розкриття даних, ніж зовнішні. Під час успішної атаки зловмисника із зовні компрометується набір однорідних даних. Наприклад, інформація з певної бази даних, що обмежена функціоналом обраної програми або системи. Але якщо розкриття даних відбулося в результаті дій співробітника компанії, то до рук зловмисника може потрапити будь-яка інформація з обмеженим доступом, що використовується й обробляється організацією. Особливо у випадку, коли працівник компанії має доступ до секретних документів або комерційної таємниці.

Також компанія InfoWatch надала статистичні дані стосовно класифікації розкриття інформації за особою, котра спровокувала інцидент інформаційної безпеки. Фрагмент цих даних наведений на рис. 1.2 [6].

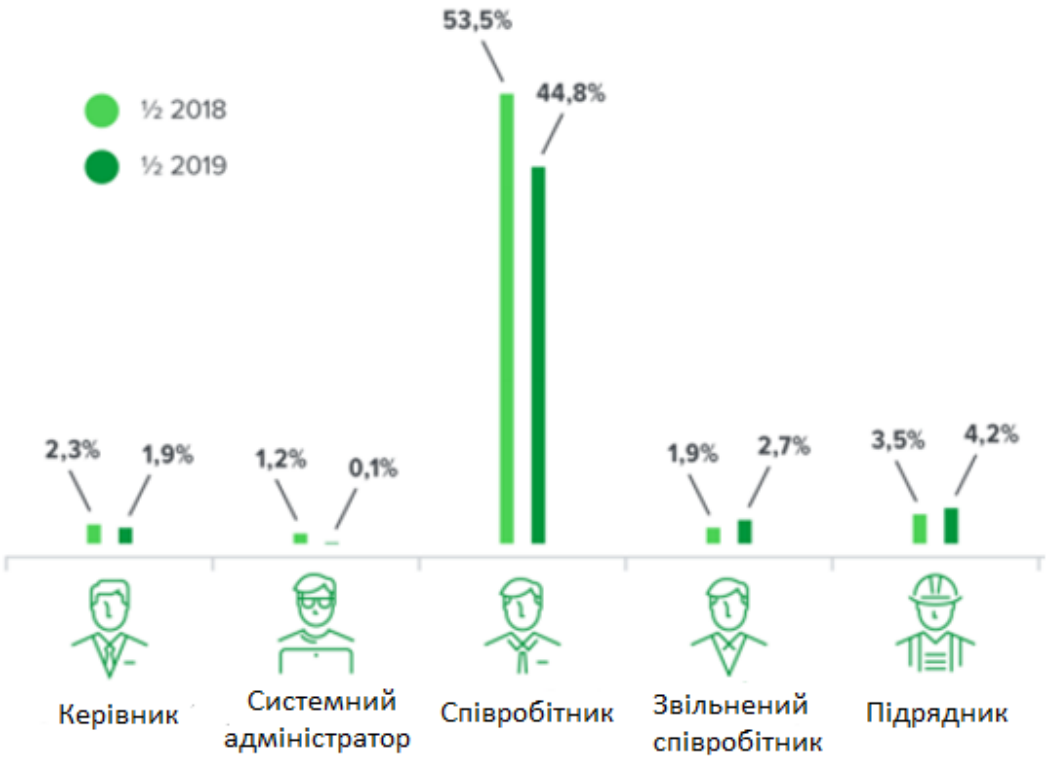

Рисунок 1.2 – Класифікація розкриття даних за особою-джерелом

Рис. 1.2 свідчить про те, що джерелом витоку інформації може бути як керуюча особа, так і звичайний співробітник. Системні адміністратори також можуть нехтувати встановленими правилами інформаційної безпеки та не до кінця виконувати свою роботу, проте більша кількість інцидентів припадає на штатних працівників.

В даному випадку метою поширення конфіденційної інформації може бути як отримання грошової винагороди, так і копіювання даних для подальшого несанкційованого використання. Проте головним рушієм є особиста вигода.

Перевірений факт, що співробітники компанії не є єдиним джерелом внутрішньої загрози витоку інформації. Промислове шпигунство ніхто не відміняв. І хоча цей вид діяльності є незаконним, деяких зловмисників це не зупиняє. До того ж деякі відомості можна добути цілком законним шляхом – запросивши на співбесіду співробітника конкурентів і задаючи спеціальні навідні запитання, можна з'ясувати деякі технічні особливості, на основі котрих можна виділити слабкі місця у інформаційній безпеці.

Також встановлено, що витік інформації з обмеженим доступом може бути і не умисним. В такому випадку йдеться про ситуації, коли внутрішній співробітник може навіть не підозрювати про можливі негативні наслідки своїх дій. Це може бути, як використання слабкого паролю для облікового запису, так і факт обговорення робочої ситуації надто голосно або при наявності сторонньої людини. Також відомі інциденти інформаційної безпеки, що відбулися через недотримання політики чистого столу. Останній варіант особливо небезпечний, якщо співробітник має високий рівень привілеїв у корпоративній мережі.

Окреме джерело розкриття конфіденційності інформаційних ресурсів становить маніпульований інсайдер. Якщо говорити про технічні засоби захисту конфіденційної інформації, то, наприклад, шляхом використання криптоаналізу можна знайти слабке місце в шифрі й скомпрометувати закодоване повідомлення. Подібну аналогію можна провести стосовно використання людського фактору – соціальні інженери можуть взаємодіяти з особливостями психології людей, щоб обійти технології захисту встановлені в компанії. Таким чином, зловмисник може обманути довірливого працівника компанії або дізнатися необхідну йому інформацію під час розмови. Також шляхом маніпуляцій соціальний інженер може отримати доступ до конфіденційних ресурсів, або створити вразливість в системі безпеки.

1.2 Канали витоку конфіденційної інформації

Згідно статистичним даним компанії InfoWatch за перше півріччя 2019 року найбільш популярними каналами витоку конфіденційних даних є мережа і електронна пошта. Про це свідчить рис. 1.3 [6].

Рисунок 1.3 – Статистика каналів витоку даних

З рис. 1.3 видно, що найбільша кількість даних компрометується через мережевий канал. У ньому 87% інцидентів інформаційної безпеки спричинені умисними діями (вони можуть включати в себе, як атаки зовнішніх зловмисників, так і активність інсайдерів) і майже 59% вважається ненавмисними (здебільшого халатність внутрішніх працівників).

Електронна пошта є другою за кількістю здійснених атак зі сторони зловмисника. Будь-який співробітник, що має корпоративну пошту може стати жертвою фішингу. Зловмиснику достатньо відправити електронний лист від імені особи або організації, яким довіряє жертва (колега по роботі, керівник чи представник партнерської компанії), з проханням перейти за посиланням. Якщо довірливий співробітник виконує описану дію, то потрапляє на підробний сайт. Всі дані, котрі йому довелося ввести потрапляють до рук шахраїв. З цього

моменту зловмисники можуть заволодіти обліковим записом співробітника і здійснювати крадіжу і поширення конфіденційних ресурсів компанії.

Також статистичні дані компанії InfoWatch свідчать про те, що ймовірність розкриття даних через «паперовий» канал зменшується, проте залишається вагомою. Тут також переважає доля ненавмисних витоків. Вони можуть бути пов’язані з винесенням документів за кордони організації, не правильною процедурою їх зберігання або знищення.

Низький показник інцидентів інформаційної безпеки серед таких каналів, як крадіжка або втрата обладнання, використання мобільних пристроїв, месенджерів, засобів передачі медіафайлів і знімних носіїв. Проте останні можуть нести значну загрозу для конфіденційних даних, якщо на основі USB підключень виникнуть приховані мережі. Даний канал витоку даних буде розглянутий більш детально у 2 розділі атестаційної роботи.

1.3 Превентивні міри запобігання витоків інформації через дії інсайдерів

Розглянуті у минулому розділі дослідження статистичних даних показали те, що інформаційні ресурси з обмеженим доступом можуть бути скомпрометовані як за допомогою зовнішніх атак, так і внутрішніх. При цьому ймовірності витоку даних обома шляхами приблизно однакова, а кількість збитків від дій інсайдерів значно більша, ніж від дій зовнішніх зловмисників. Тому керівництву компанії варто приділяти особливу увагу запобіганню інцидентів інформаційної безпеки через вину штатних працівників.

Для організації достатнього рівня інформаційної безпеки необхідно ввести поняття «соціального брандмауера» [7]. Цей термін поєднує в собі сукупність організаційних заходів інформаційної безпеки, спрямованих на роботу з персоналом. Під час розробки цих заходів, необхідно спиратися на стандарт ISO 17799. У ньому наведені основні принципи і правила управління персоналом з урахуванням вимог інформаційної безпеки. Ці рекомендації зводяться до необхідності виконання певних вимог при наймі та звільненні працівників, підвищення обізнаності та застосування запобіжних заходів до порушників. Дотримання цих правил дозволяє істотно знизити вплив людського фактору, уникнути характерних помилок і, в багатьох випадках, запобігти витоку інформації або відкинути можливість її неналежного використання.

Також з практичної точки зору, стандарт ISO 17799 може застосовуватися як засіб аудиту системи інформаційної безпеки. Існують певні програмні продукти, котрі реалізовані на основі цього стандарту. Наприклад, таке програмне забезпечення, як COBRA ISO 17799 Consultant, надає можливість проведення аудиту у вигляді анкетування. Цей процес можна представити у вигляді чотирьох послідовних етапів:

– анкетування – заповнення анкет одним або декількома співробітниками, відповідальними за забезпечення інформаційної безпеки;

– визначення елементів, що відповідають висунутим в стандарті вимогам до системи інформаційної безпеки;

– виявлення ресурсів, які потребують додаткового захисту (так званих «слабких місць»);

– отримання рекомендацій щодо підвищення рівня захисту для виявлених на попередньому етапі ресурсів.

Після проведення подібного аудиту можна зробити висновки про існуючу систему інформаційної безпеки, проаналізувати обізнаність і проінформованість робочого персоналу стосовно неї і виокремити шляхи її покращення.

Окрім цього, надійний “соціальний брандмауер” повинен будуватися на фундаменті політики інформаційної безпеки. В організації необхідно розробити положення щодо захисту конфіденційної інформації та відповідні інструкції. Ці документи повинні визначати правила і критерії для категорування інформаційних ресурсів за ступенем конфіденційності, правила маркування і поводження з конфіденційною інформацією. Також необхідно приділити увагу правилам надання доступу до інформаційних ресурсів, впровадженню відповідних процедур і механізмів контролю, включаючи авторизацію і аудит доступу.

Важливе місце повинна посідати процедура роботи з неактуальними акаунтами. До них відносяться облікові записи осіб, що більше не працюють в організації. Маючи можливість підключення до корпоративної мережі, вони можуть здійснювати деструктивні дії, що можуть стати основою інцидентів інформаційної безпеки. Окрім цього, необхідно розробити систему блокування облікових записів співробітників, котрі перебувають у відпустці або на лікарняному, оскільки зловмисники також можуть скористатися можливістю і використовувати акаунти у своїх цілях.

Взагалі корпоративна мережа являє собою канал обміну інформаційними даними, завдяки якому працівники організації мають безперервний доступ до всіх ресурсів компанії. Саме тому у наступних розділах атестаційної роботи будуть розглянуті механізми пошуку інсайдерів у корпоративних мережах і способи противодії їм.

Окрему роль в мінімізації витоків інформації через вину штатного працівника займають системи предиктивної аналітики. Згідно з даними компанії InfoWatch, інструменти цих систем здатні прогнозувати вірогідність виникнення у співробітників намірів здійснити звільнення чи перейти на бік конкурентів. В подібних ситуаціях штатний працівник може перетворитися в інсайдера, котрий своїми діями здатний модифікувати, поширювати або взагалі видаляти цінні інформаційні ресурси компанії.

Соціальний міжмережевий екран дозволяє успішно боротися з найбільш численним класом загроз – ненавмисне розголошення конфіденційної інформації, але для боротьби зі зловмисниками його недостатньо. Для того щоб зупинити інсайдера, котрий навмисно поширює інформацію з обмеженим доступом, необхідно додатково задіяти різноманітні програмно-технічні механізми захисту.

1.4 Пропозиції щодо організації структури корпоративної мережі, в котрій можна буде виявити інсайдера

У підрозділі 1.2 було встановлено, що найбільша кількість витоків конфіденційних даних відбувається через корпоративні мережі. Саме тому безпечна взаємодія з конфіденційними даними потребує правильної побудови і налагодження корпоративної мережі. Розумно складена топологія мережі забезпечить організацію швидкісного і захищеного каналу передачі даних, завдяки якому співробітники отримають безперервний доступ до всіх ресурсів мережі і периферійних пристроїв.

Також обдумане розгортання корпоративної мережі на підприємстві дозволить організувати:

- швидкий процес обробки даних;
- оперативне інформування працівників і реагування на зміни;
- моментальний доступ до всієї корпоративної інформації в режимі реального часу;

- можливість спільного використання даних і пристроїв;
- підвищення ефективності комунікації між співробітниками і налагодження бізнес-процесів;
- електронний документообіг, створення електронних архівів;
- захист даних від несанкціонованого доступу ззовні;
- максимальну гнучку і масштабовану систему управління підприємством.

Комп'ютерні потреби більшості невеликих організацій можуть бути задоволені за допомогою однієї локальної мережі з одним або двома серверами, котрими зазвичай може керувати одна людина, що володіє лише помірними технічними знаннями і досвідом. Якщо ж корпоративна мережа обслуговує декілька географічних місць і декілька будівель в кожному з них, то необхідно задіяти більше технічних можливостей і висококваліфікованих системних адміністраторів.

У середніх і великих компаніях, в котрих кількість робочих станцій сягає більше 20, пропонується використання мережі з контролером домену з розгорнутою роллю Active Directory Domain Service. Також ця архітектура мережі підійде для компаній, котрі мають географічно розгалужені філіали або віддалених працівників. Це все зумовлено тим, що Active Directory являє собою каталог, в котрому зберігається інформація про мережеві ресурси і служби, котрі надають доступ до цієї інформації. Завдяки цьому, використання AD DS може забезпечити наступні можливості:

- полегшене адміністрування;
- масштабованість корпоративної мережі;
- підтримка відкритих стандартів;
- підтримка стандартних форматів імен.

Служби AD DS слугують фундаментом для кожної доменної мережі Windows. Вони дають можливість зберігати інформацію про членів домену, включаючи пристрої та користувачів, перевіряти їхні облікові дані та визначати їхні права доступу. Все це реалізується за допомогою протоколу Kerberos і технології Single Sign-On (SSO). Kerberos перевіряє справжність облікових даних і видає користувачеві квиток, за допомогою якого користувач отримує доступ до ресурсів і служб, які підтримують Kerberos. Сервер, на якому працюють ці

механізми, називається контролером домену. Також для повної інтеграції на даний сервер дуже часто встановлюють служби DHCP і DNS.

Домен Active Directory являє собою групу комп'ютерів, котрі спільно використовують загальну базу даних каталогу. У свою чергу, ця база даних зберігається на виділених серверах – контролерах домену. Вони реплікують розділ сховища даних, який містить дані ідентифікації користувачів, груп і комп'ютерів домену. Це дозволяє реалізувати мережевий вхід в систему на всіх робочих станціях підприємства. Домени в Active Directory виступають в якості кордонів адміністративної безпеки об'єктів і містять свої власні політики безпеки

Служби Active Directory мають широкі можливості масштабування. У лісі Active Directory може бути створено понад 2-х мільярдів об'єктів. Це дозволяє впроваджувати службу каталогів в компаніях з сотнями тисяч комп'ютерів і користувачів. Ієрархічна структура доменів дозволяє гнучко масштабувати IT-інфраструктуру на всі філії та регіональні підрозділи компаній. Для кожної філії або підрозділу компанії може бути створений окремий домен, зі своїми політиками, своїми користувачами і групами. Для кожного дочірнього домену можуть бути делеговані адміністративні повноваження місцевим системним адміністраторам. При цьому все одно дочірні домени підкоряються батьківським. На рис. 1.4 представлений варіант побудови мережі з використанням служб AD.

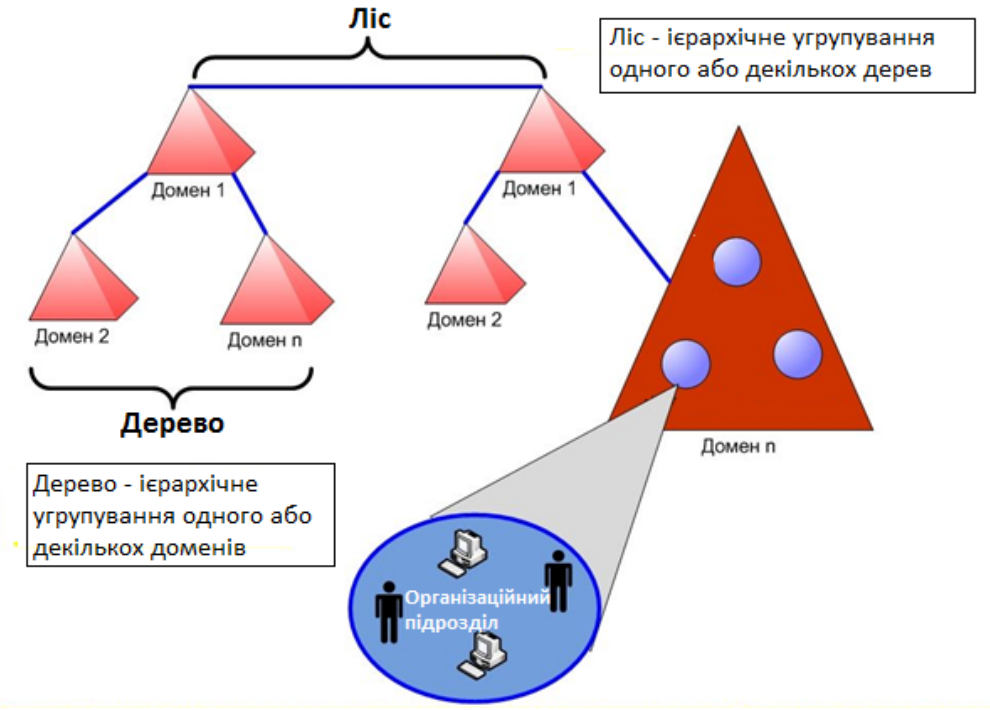

Рисунок 1.4 – Мережа зі службами Active Directory

У розрізі перерахованих можливостей Active Directory також можна виділити і основні завдання, на виконання яких націлена служба каталогів:

– зберігання інформації про об'єкти мережі та надання її користувачам і системним адміністраторам;

– представлення мережі в інтуїтивно зрозумілому ієрархічному вигляді і централізоване управління всіма об'єктами мережі;

– підвищення ступеню інформаційної безпеки за рахунок розмежування адміністративних повноважень обслуговуючого персоналу і впровадження сучасних методів захисту інформації;

– проектування єдиної структури каталогу, яка забезпечить прозоре використання інформаційних ресурсів в рамках компанії.

Крім того, можливості служби Active Directory дозволяють налаштувати довірчі відносини між доменними лісами. Кожна компанія має власний ліс доменів, кожен з яких має власні ресурси. Але на практиці системний адміністратор може зіштовхнутися з ситуацією, коли необхідно надати доступ до своїх корпоративних ресурсів співробітникам іншої компанії – робота з загальними документами і додатками в рамках спільного проекту. Для цього між лісами організацій можна налаштувати довірчі відносини, що дозволить співробітникам однієї організації авторизуватися в домені іншої.

Отже, правильне розгортання доменних служб Active Directory дозволить використати всі переваги централізованої делегованої моделі управління і можливості єдиного входу. Проте, якщо в корпоративних мережах подібного типу співробітники продовжують використовувати знімні носії інформації, то на основі цих USB підключень можуть виникнути приховані мережі.

Поняття прихована мережа включає в себе процес міграції знімного носія від одного комп’ютеру до іншого. Таким чином, конфіденційна інформація може потрапити у інший філіал або підрозділ компанії, котрий має менший рівень захисту або у якому працівники за замовчуванням не повинні мати доступ до вказаних інформаційних ресурсів.

Виникнення прихованої мережі підвищує ризик компрометації даних. У наступному розділі атестаційної роботи даний канал витоку інформації буде розглянутий більш детально.

2 АНАЛІЗ ПІДХОДІВ ЩОДО ВИЯВЛЕННЯ ПРИХОВАНИХ МЕРЕЖ

Як згадувалось у першому розділі атестаційної роботи, поняття прихованої мережі пов’язано з підключенням одного USB-пристрою до декількох робочих комп’ютерів. У такий спосіб конфіденційні дані можуть мігрувати не лише між організаційними підрозділами компанії, а й між її філіалами.

Відомо, що контроль усіх інформаційних ресурсів компанії – важкий процес, що потребує неабияких ресурсів і спеціального планування. Тому в компаніях прийнято проводити категорування інформації та, в залежності від ступеня її секретності, визначати міри захисту, способи доступу до даних і осіб, котрі можуть здійснювати їх обробку.

Відповідно до цього, різні організаційні підрозділи (групи) компанії можуть мати різні рівні інформаційної безпеки. Саме тому мігрування даних в межах компанії може становити загрозу. Якщо конфіденційні дані потраплять в незахищений простір, то й відповідно збільшиться ймовірність компрометації цих даних.

Проблема прихованих мереж підтверджує актуальність витоків інформаційних ресурсів через вину штатних співробітників компанії. Переміщення конфіденційних даних між різними організаційними структурами компанії відбувається через людський фактор. Також існує ймовірність, що персонал може бути не достатньо проінформований про процедури обробки і взаємодії з інформацією з обмеженим доступом, внаслідок чого дані можуть бути скомпрометовані.

Найпростіший спосіб вирішення проблеми прихованих мереж – заборона використання USB-накопичувачів і блокування USB портів. Проте, цей варіант важко назвати гнучким, оскільки, наприклад, більшість сучасних пристроїв введення-виведення (наприклад, маніпулятор «миша») підключається саме через USB. Також ніяка компанія не застрахована від того, що в корпоративній мережі може статися збій, а інформаційні ресурси необхідно буде передати в інший підрозділ чи роздрукувати – тоді їх прийдеться скопіювати на USB, щоб передати необхідній уповноваженій особі. Тож проблема залишається актуальною і потребує вирішення.

Розглянемо більш ефективні методи виявлення прихованих мереж та їх контролю.

2.1 Використання спеціального програмного забезпечення

Сучасні технології дозволяють організувати надійний захист і моніторинг корпоративної мережі на основі використання спеціального програмного забезпечення класу Data Leak Prevention (DLP). Ці системи здійснюють аналіз потоків даних, які перетинають периметр захищеної інформаційної системи. При виявленні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи і передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак, наприклад, грифа документа, спеціально введених міток чи значень хеш-функцій. Таким чином, подібний програмний продукт може вирішити проблему неправомірного копіювання інформації з робочих комп'ютерів на флеш-накопичувачі, смартфони, планшетні комп'ютери та інші носії даних.

В даній атестаційні роботі були досліджені можливості програмного продукту DeviceLock DLP.

DeviceLock DLP – система захисту конфіденційних даних, шо розробляється з 1996 року компанією SmartLine Inc. Для захисту від витоків інформації цей програмний продукт використовує повнофункціональний набір контекстних і контентно-залежних механізмів ефективного контролю використовуваних (data-in-use), переданих (data-in-motion) і збережених (data-at-rest) даних.

Сервер і виконавчі агенти DeviceLock Discovery забезпечують превентивний захист від потенційних витоків інформації за допомогою заданих адміністратором автоматичних дій щодо усунення виявлених порушень, а також ініціювання процедур управління інцидентами за допомогою оперативних тривожних сповіщень, що відправляються персоналу служб інформаціної безпеки.

Отже, правильне налаштування цього програмного забезпечення допоможе не тільки уникнути виникнення прихованих мереж, а й контролювати їх. Оскільки функціонал цього програмного продукту дозволяє створити «білий список» пристроїв, котрі можуть бути підключені до робочої станції. На рис 2.1 представлений приклад використання цього програмного забезпечення.

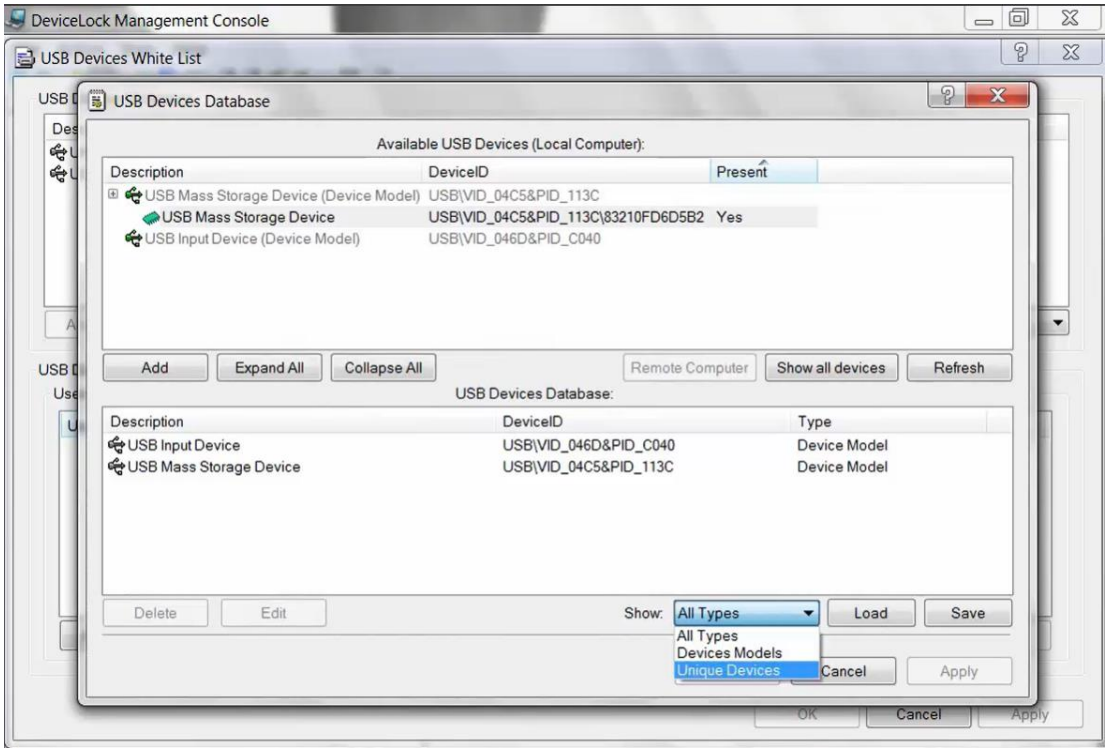

Рисунок 2.1 – Створення «білого списку» в DeviceLock Management Console

При підключені до комп’ютеру не включених до переліку дозволених USB-пристроїв, система буде формувати сповіщення. За унікальним серійним номером USB-накопичувача або за комп’ютером, з якого надійшло тривожне повідомлення можна ідентифікувати недобросовісного працівника, котрий хотів порушити встановлені норми інформаційної безпеки, або ж активного зловмисника. Також DeviceLock виявляє USB-кейлоггери і блокує клавіатури, котрі під'єднані до них.

Ще однією можливістю DeviceLock є контроль синхронізації комп'ютера з смартфонами і здійснення аудиту та тіньового копіювання даних, що передаються з комп'ютера на ці мобільні пристрої. Тобто після створення «білого списку» USB-пристроїв можна також вислідити які дані були записані на ці пристрої.

DeviceLock DLP дозволяє службам інформаційної безпеки централізовано і оперативно управляти DLP-політиками в масштабах всієї організації незалежно від розміру IT-інфраструктури. Це досягається завдяки інтеграції управління в групові політики домену Microsoft Active Directory і вбудуванню консолі DeviceLock в оснастку управління Microsoft Group Policy Management Console (GPMC). Крім того, DeviceLock підтримує будь-які LDAP-каталоги, робочі групи і може використовуватися на відокремлених від загальної мережі робочих

станціях під керуванням Windows, забезпечуючи повний контроль мобільних співробітників.

На рис. 2.2 зображені сфери дії DeviceLock в мережі з установленими ролями Active Directory.

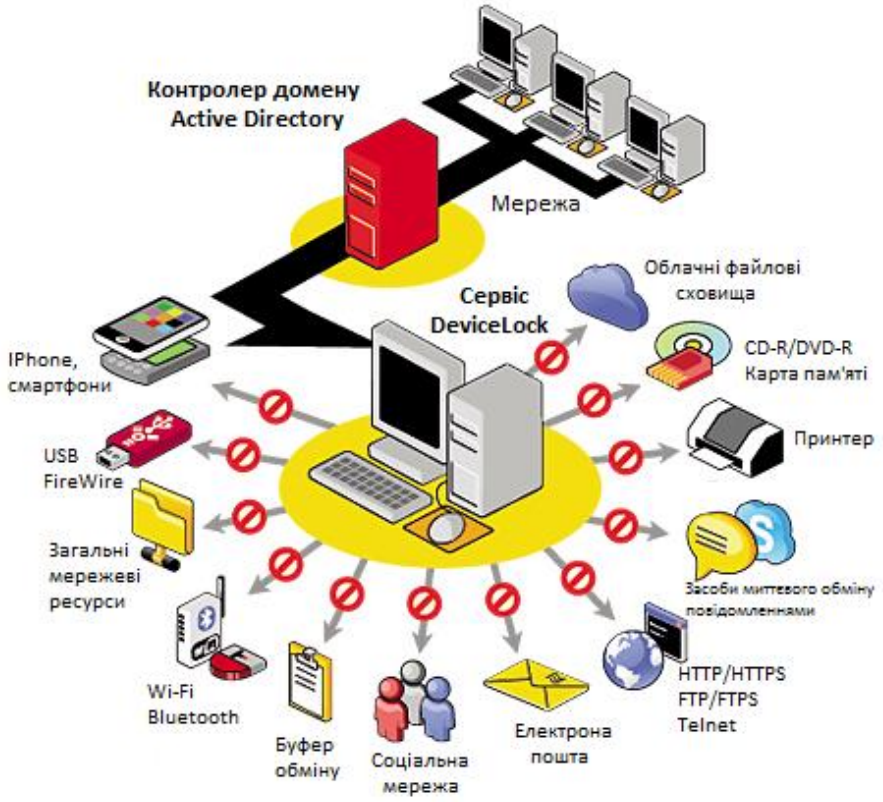

Рисунок 2.2 – Сфери дії DeviceLock при інтеграції в мережу з контролером домену Active Directory

Також для захисту корпоративної мережі від інсайдерських атак можна використовувати концепцію IPC (Information Protection and Control). ЇЇ сенс полягає в об'єднанні методів DLP і шифрування. Тобто за допомогою програмного забезпечення класу DLP контролюється інформація, що покидає межі корпоративної мережі по технічним каналам, а шифрування – використовується для захисту носіїв даних, які фізично потрапляють або можуть потрапити в руки сторонніх осіб.

Отже технологія IPC є логічним продовженням технології DLP і дозволяє захищати дані не тільки від витоків технічними каналами, тобто інсайдерів, але і від несанкціонованого доступу користувачів до мережі, інформації, додатків і в тих випадках, коли безпосередньо носій інформації потрапляє в руки третіх осіб. Наприклад, діставши жорсткий диск з персонального комп'ютера, інсайдер не

зможе прочитати записану на нього інформацію, оскільки вона буде зберігатися у зашифрованому вигляді. Це дозволяє не допустити компрометацію конфіденційних даних навіть у разі втрати, крадіжки або вилучення (наприклад, при організації оперативних заходів фахівцями спецслужб, недобросовісними конкурентами або рейдерами).

Розглянемо найбільш поширені технології шифрування, які можуть застосовуватися в концепції IPC.

1) Шифрування знімних носіїв. Незважаючи на архаїчність цього типу носія, він продовжує активно використовуватися для резервного копіювання та для перенесення великих обсягів інформації. Відповідно втрата таких носіїв інформації може нести серйозну загрозу для інформаційної безпеки. Ситуація ускладнюється тим, що USB-накопичувачі можуть містити великі обсяги даних, а отже велика кількість людей може стати жертвами шахраїв.

2) Шифрування серверних сховищ. Незважаючи на те, що серверні сховища дуже рідко транспортують, і ризик їх втрати все рівно нижче, ніж у знімного накопичувача, окремий жорсткий диск зі сховища може потрапити в руки зловмисників. Ремонт, утилізація, апгрейд – ці події виникають з достатньою регулярністю для того, щоб списувати цей ризик з рахунків. Та й ситуація проникнення в офіс сторонніх осіб не є абсолютно неможливою подією.

Якщо в корпоративний мережі використовується RAID (Redundant Array of Independent (or Inexpensive) Disks), як спосіб зберігання одних і тих же даних у різних місцях на декількох жорстких дисках або твердотільних накопичувачах для захисту даних у разі відмови накопичувача. То все одно не потрібно нехтувати шифруванням, оскільки ніяка компанія не застрахована від того, що один із елементів може потрапити в сторонні руки.

Здавалося б, чергування записуваних даних на кілька жорстких дисків, яке виконують контролери RAID, забезпечує зберігання даних у вигляді, котрий буде важко прочитати зловмиснику. На жаль, це не зовсім так. Чергування дійсно має місце, однак в більшості сучасних пристроїв воно виконується на рівні блоків по 512 байт. Це означає, що, незважаючи на порушення структури і форматів файлів, конфіденційну інформацію витягти з такого жорсткого диска все одно можливо. Тому, якщо поставлено вимогу щодо забезпечення конфіденційності інформації при її зберіганні в RAID-масиві, єдиним надійним варіантом залишається шифрування.

Також необхідно здійснювати шифрування ноутбуків, оскільки втрата або крадіжка ноутбуків з конфіденційною інформацією вже котрий рік не виходять з першої п'ятірки найпопулярніших інцидентів інформаційної безпеки.

Якщо в існуючій корпоративній мережі шифрування ноутбуків буде здійснюватися на ряду з шифруванням знімних накопичувачів, то у цьому випадку говорять про свого роду кріптопериметр, який забезпечує автоматичне прозоре шифрування носіїв всередині, і неможливість розшифрування даних за його межами.

Обов'язковою компонентом IPC є архів, який ведеться для обраних потоків інформації (пакетів, повідомлень). Вся інформація про дії співробітників зберігається в одній або декількох пов'язаних базах даних. Лідируючі IPC-системи дозволяють архівувати всі канали витоку, які вони можуть контролювати. В архіві IPC зберігаються копії поширених в інтернеті документів і тексту, електронних листів, роздрукованих документів і файлів, записаних на периферійні пристрої. У будь-який момент адміністратор інформаційної безпеки може отримати доступ до будь-якого документу або тексту в архіві, використовуючи лінгвістичний пошук інформації за єдиним архівом (або за всіма розподіленим архівами одночасно). Будь-які повідомлення при необхідності можна подивитися або переслати, а будь-який завантажений в Інтернет, записаний на зовнішній пристрій або роздрукований файл або документ переглянути або скопіювати. Це дозволяє проводити ретроспективний аналіз можливих витоків конфіденційних даних.

Таким чином, шифрування може істотно розширити можливості DLP-систем і знизити ризики витоку конфіденційних даних. Незважаючи на те, що концепція IPC виникла порівняно недавно, і вибір комплексних IPC-рішень на ринку не дуже широкий, індустрія активно освоює цю сферу і цілком можливо, що через деякий час ця концепція стане стандартом де-факто для вирішення проблем внутрішньої безпеки і внутрішнього контролю.

Використання спеціального програмного забезпечення класу DLP – це оптимальний і гнучкий варіант побудови захищеної корпоративної мережі, проте при використанні сторонніх програм завжди існує загроза експлойту. Системний адміністратор не може гарантувати, що десь у реалізації програмного забезпечення не прихований шкідливий програмний код, котрий може завдати шкоди корпоративній IT інфраструктурі. Саме тому для організації інформаційної безпеки підприємства краще використовувати штатні засоби операційної системи.

Розглянемо можливості Microsoft Windows Server з розгорнутими ролями Active Directory.

2.2 Використання штатних засобів Active Directory для виявлення прихованих мереж

Підключення USB-накопичувача до робочого комп'ютера зазвичай пов'язується з фіксуванням в системі даних про цей пристрій. На основі аналізу цих даних можна знайти приховану мережу і сам пристрій, через котрий вона виникла.

Під час першого підключення знімного USB носія відбувається установка драйвера пристрою. Диспетчер введення-виведення створює об'єкт «драйвер» і записує в його атрибути точки входу. Також в системі фіксується Vendor ID (ідентифікатор виробника), Product ID (ідентифікатор продукту) і серійний номер. Ці дані допомагають ідентифікувати пристрій в системі і розпізнати його при підключенні наступного разу. Також під час установки драйвера пристрою формується унікальний GUID (Globally Unique Identifier). У системі він відображається у вигляді послідовності 32 шістнадцятирічних цифр, що розділені дефісом. Наприклад, на рис. 2.3 відображений GUID для USB-накопичувача, підключеного до системи – {eec5ad98-8080-425f-922a-dabfde3f69a}.

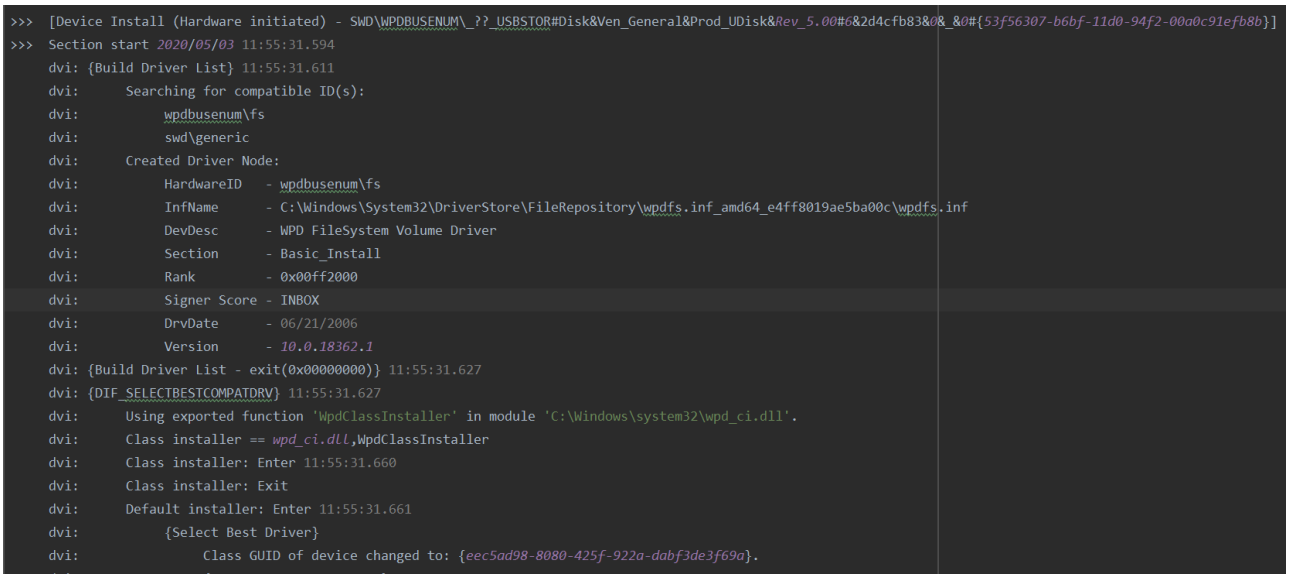

Рисунок 2.3 – Інформація про USB-пристрій, котра зафіксована у журнальному файлі операційної системи

Найлегший спосіб відслідкувати які пристрої підключалися до робочого комп'ютера – це дослідження лог-файлів операційної системи. На рис. 2.4 відображений фрагмент журнального файлу setupapi.dev.log. У ньому зафіксоване нове підключення до системи, назва пристрою (поле DevDesc), а також дата і час цієї події.

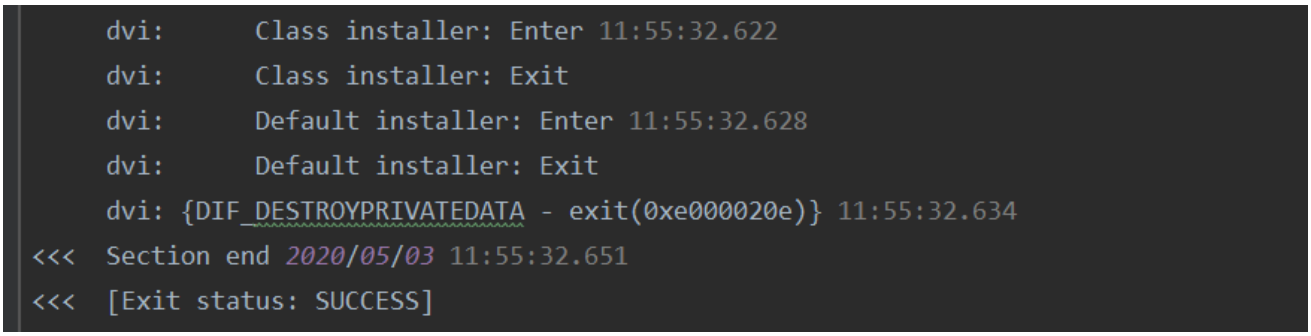

Рисунок 2.4 – Перегляд статусу підключення нового USB-пристрою у файлі setupapi.dev.log

Тобто якщо взяти декілька робочих станцій і порівняти лог-файли, то можна виявити підключення одного й того ж пристрою, а на основі часу підключення можна зробити висновки стосовно напрямку переміщення інформаційних ресурсів в корпоративній мережі.

Також на рис. 2.3 видно, що спочатку створюється драйвер для підключеного пристрою (про це свідчить рядок з "Created driver node") і йому присвоюється HardwareID. Цей ідентифікатор повідомляє Windows, який драйвер потрібно використовувати для пристрою, коли він буде підключений наступного разу. З асоціюванням HardwareID одночасно відбувається створення унікального ідентифікатора GUID.

Також у setupapi.dev.log фіксуються як вдалі підключення нових пристроїв, так і ні. Наприклад на рис. 2.4 останній рядок показує, що підключення було вдалим, а, отже ця подія може нести ризик для інформаційної безпеки.

Наступний ресурс, котрий може допомогти системному адміністратору виявити приховану мережу, – це системний реєстр. У ньому також фіксуються підключення усіх USB-пристроїв, що пройшли процедуру створення драйвера. До переваг дослідження цього ресурсу можна віднести те, що інформація надається у більш структурованому і розгорнутому вигляді.

Для перегляду системного реєстру використовується утиліта regedit.exe, котра відкриває Registry Editor.

Події, пов’язані з USB-пристроями, фіксуються у гілках USB і USBSTOR. Перша містить інформацію стосовно всіх USB-підключень, а друга лише стосовно флеш-накопичувачів. Знайти ці гілки можна за наступним шляхом: HKLM\System\CurrentControlSet\Enum.

На рис. 2.5 здійснений перегляд даних у гілці USB ключа HKEY_LOCAL_MACHINE. Якщо порівняти з гілкою USBSTOR, котра представлена на рис. 2.6, то тут зафіксовано набагато більше підключень. Оскільки тут фіксується підключення до системи смартфонів, USB-камер та маніпуляторів «миша».

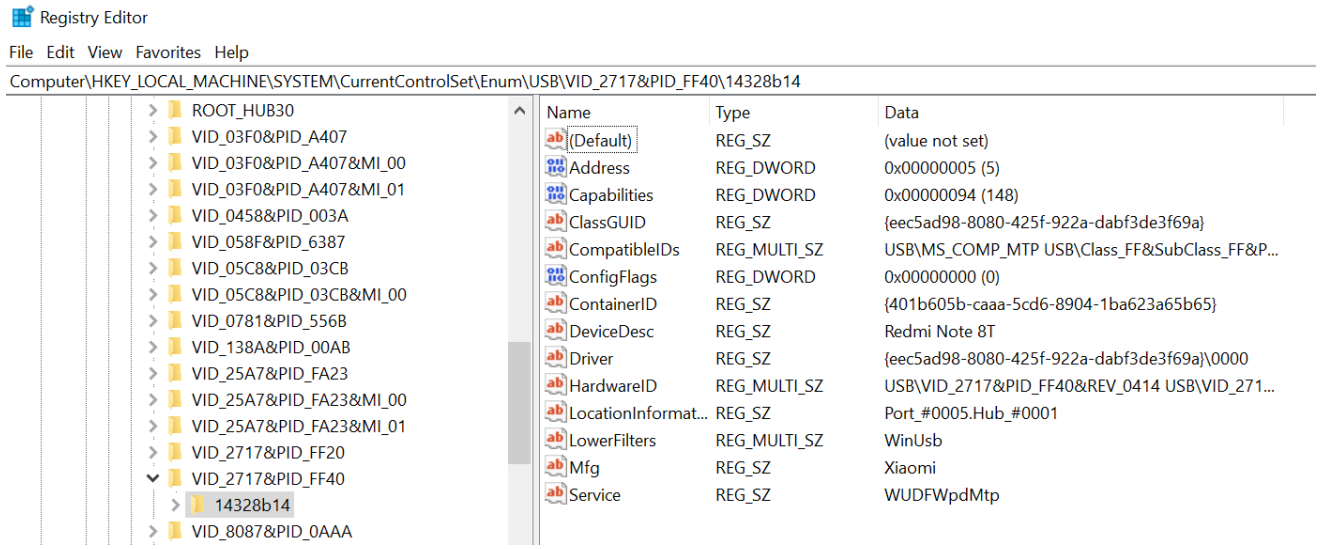

Рисунок 2.5 – Гілка реєстру USB

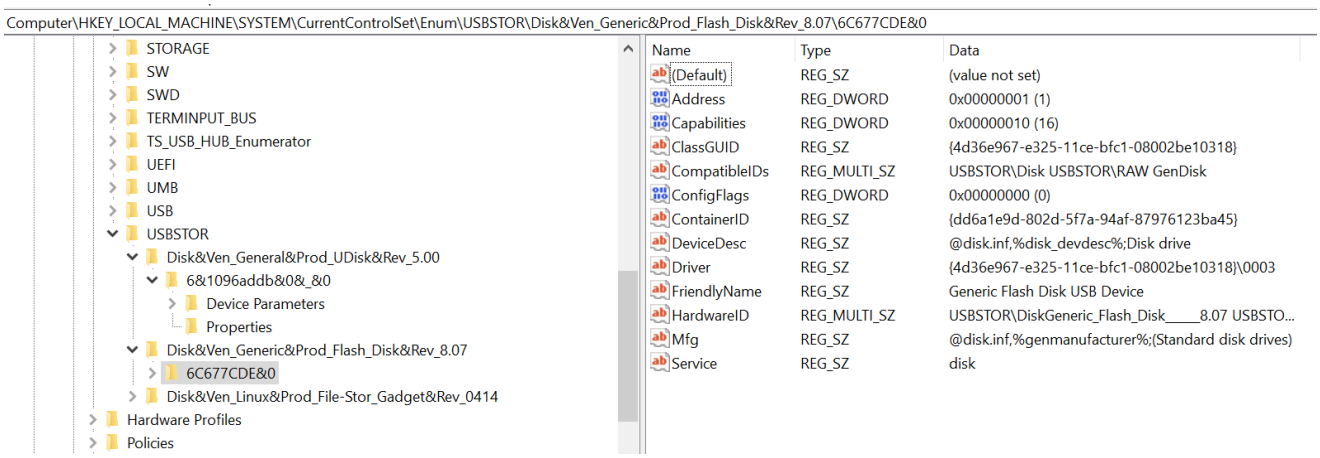

Рисунок 2.6 – Гілка реєстру USBSTOR

Рис. 2.5 показує, що кожне нове підключення асоціюється зі створенням в реєстрі директорії з назвою на основі Vendor ID і Product ID. Далі ця директорія має вкладеність у вигляді ще однієї директорії, назва котрої є серійними номером пристрою.

У USBSTOR іменування директорій містить трохи іншу логіку. Назва верхньої директорії складається з імені постачальника, імені продукту і його версії. Кожна складова відділена від попередньої амперсантом. Це видно з рис. 2.6. Далі, у нижній директорії розташовані параметри, котрі дають можливість однозначно ідентифікувати USB-пристрій і використати цю інформацію, щоб виявити приховану мережу, оскільки порівнявши системний реєстр комп'ютерів, що входять в одну корпоративну мережу, можна виявити екземпляри, що пов'язані зв'язком на основі USB-підключень. На рис. 2.7 наведений приклад прихованої мережі.

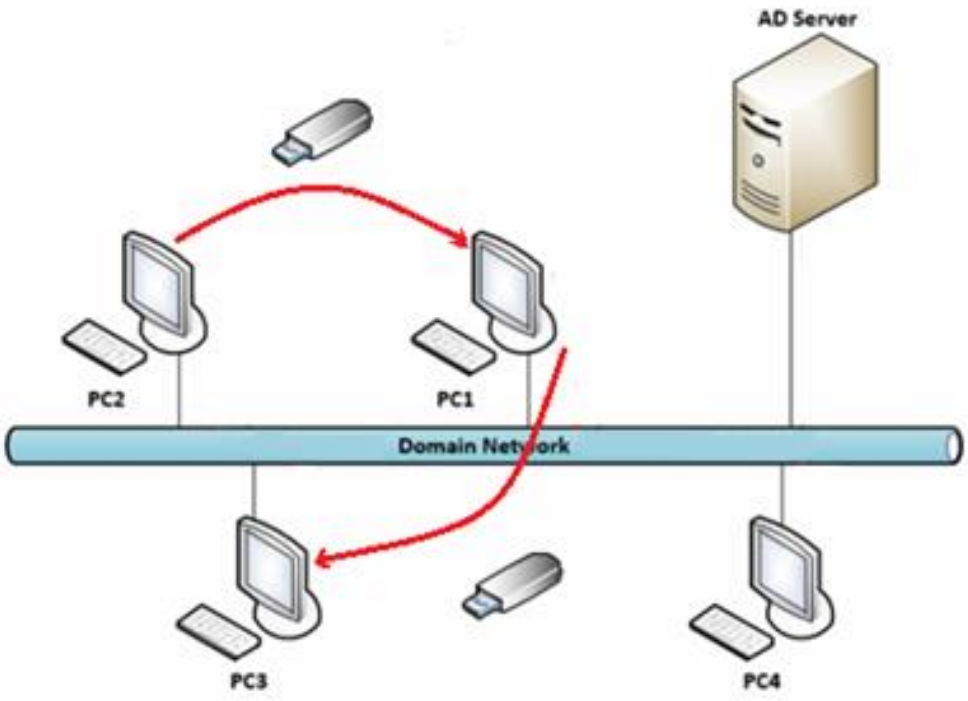

Рисунок 2.7 – Приклад прихованої мережі на основі USB-підключень

Проте, дослідження лог-файлів або системного реєстру – це дуже трудомісткий та довгий процес. Особливо, якщо корпоративна мережа включає в себе велику кількість робочих комп'ютерів. В такому випадку оптимальним рішенням буде написання і використання спеціальних скриптів. Вони будуть автоматизовано виконувати пошук прихованих мереж. Для цього системному

адміністратору необхідно буде запустити на центральному вузлі мережі (контролері домену) програмне забезпечення і воно відпрацює на всіх користувацьких комп’ютерах.

Щоб втілити в життя цей механізм пошуку прихованих мереж, необхідно активувати на кожному комп’ютері мережі скрипт Windows Remote Management (WinRM). Це дозволить віддалено застосувати запуск потрібних команд оболонки PowerShell. Таким чином, можна буде здійснити аудит навіть тих робочих станцій, що знаходяться за межами офісу або в іншому місті.

Для того, щоб налаштувати WinRM, необхідно виконати команду winrm quickconfig.

Після того, як системний адміністратор переконається у тому, що на кожному комп’ютері налаштовані служби Windows Remote Management, можна переходити до запуску скрипта. На рис. 2.8 наведений фрагмент використання скрипта.

Рисунок 2.8 – Процес запуску скрипта для пошуку прихованих мереж

Скрипт LaunchUSBHiddenNetworks виконує підключення до всіх корпоративних робочих станцій і аналізує данні стосовно USB-підключень. Для моніторингу USB використовується скрипт RecollectUSB, котрий викликається в коді основного скрипта. Це зроблено з метою розділення відповідальності частин коду і підвищення його структурованості. Розроблені скрипти надані у Додатку А та Додатку Б.

Внаслідок цих маніпуляцій, системний адміністратор отримає інформацію у вигляді короткого звіту по кожному з підключених до корпоративної мережі комп’ютерів. Цей звіт наведений на рис. 2.9.

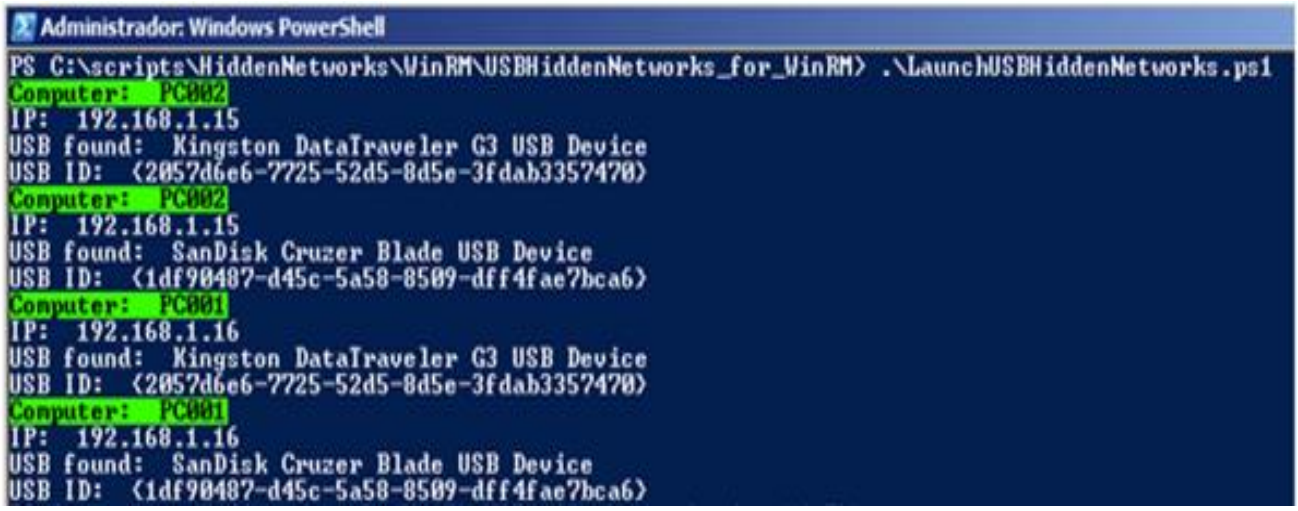

Рисунок 2.9 – Дані, котрі отримані внаслідок роботи запропонованого скрипта для аудиту корпоративної мережі

З рис. 2.9 видно, що на момент експерименту було виявлено USB підключення до кожного з комп’ютерів. Однак, варто приділити увагу тому, що між 1 і 2 комп’ютером є зв’язок у вигляді використання одного і того ж знімного носія. Тобто обидві робочі станції спільно використовували два USB-накопичувача.

Проаналізувавши всі дані, котрі були отримані в результаті відпрацювання вказаного скрипта, вдалося побудувати схему прихованої мережі. Схема мережі наведена на рис. 2.10.

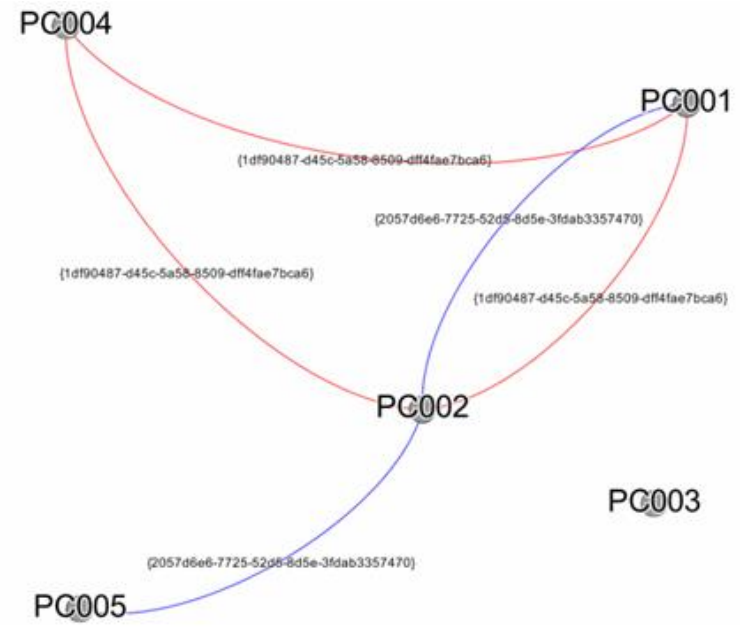

Рисунок 2.10 – Схема виявлених прихованих мереж

Якщо розглянути схему виявлених мереж, що зображена на рис. 2.10, то можна побачити 2 приховані мережі. Кожна з них виділена окремим кольором. Під найбільшою загрозою компрометації знаходяться інформаційні ресурси, що обробляються і зберігаються на вузлі №002, оскільки даний елемент корпоративної мережі одночасно входить до складу двох прихованих мереж. Також це стосується і комп'ютера з номером 001.

Найменша загроза розкриття даних через використання USB-підключень прослідковується на комп'ютері №003. Хоча там і було зафіксоване використання USB, проте не була зафіксована прихована мережа. Це може свідчити про те, що працівник, використовує знімні носії у відповідності до всіх вимог інформаційної мережі, або навпаки можливе підключення до комп'ютера не з діапазону корпоративної мережі. Тоді це становитиме ще більшу загрозу конфіденційності інформаційних ресурсів.

Таким чином постає питання не тільки виявлення прихованих мереж, а й їх контролю. Для вирішення цієї проблеми також раціонально використовувати вбудовані можливості операційної системи. Якщо говорити про корпоративну мережу з розгорнутими ролями Active Directory, то найбільш результативним буде використання групових політик.

Групові політики Active Directory дозволяють організувати гнучкий контроль корпоративної мережі [8]. За допомогою них можна налаштувати централізований контроль налаштувань на клієнтських комп'ютерах і серверах, підключених до домену, а також забезпечити простий спосіб поширення програмного забезпечення.

Тож, якщо говорити про приховану мережу, що виникла на основі USB-підключень, то системний адміністратор може використати групові політики для того, щоб заборонити підключення до робочих комп'ютерів сторонніх флеш накопичувачів. Це може бути корисно, якщо на підприємстві існують певні знімні носії, до котрих приміняється шифрування та інші засоби безпеки. Тоді можна задати список дозволених USB-пристроїв в налаштуваннях групових політик і мінімізувати ризик компрометації даних.

Для того, щоб втілити в життя цей сценарій, системному адміністратору необхідно буде відкрити Редактор групових політик і перейти в Computer Configuration, а далі в Administrative Templates. Там можна буде знайти

директорію з назвою System. В ній міститься ціла ієрархія директорій, котрі містять певні налаштування групових політик.

В контексті даного випадку нас цікавлять Driver Installation і Device Installation [9]. На рис. 2.11 наведена політика Driver Installation і декілька її параметрів.

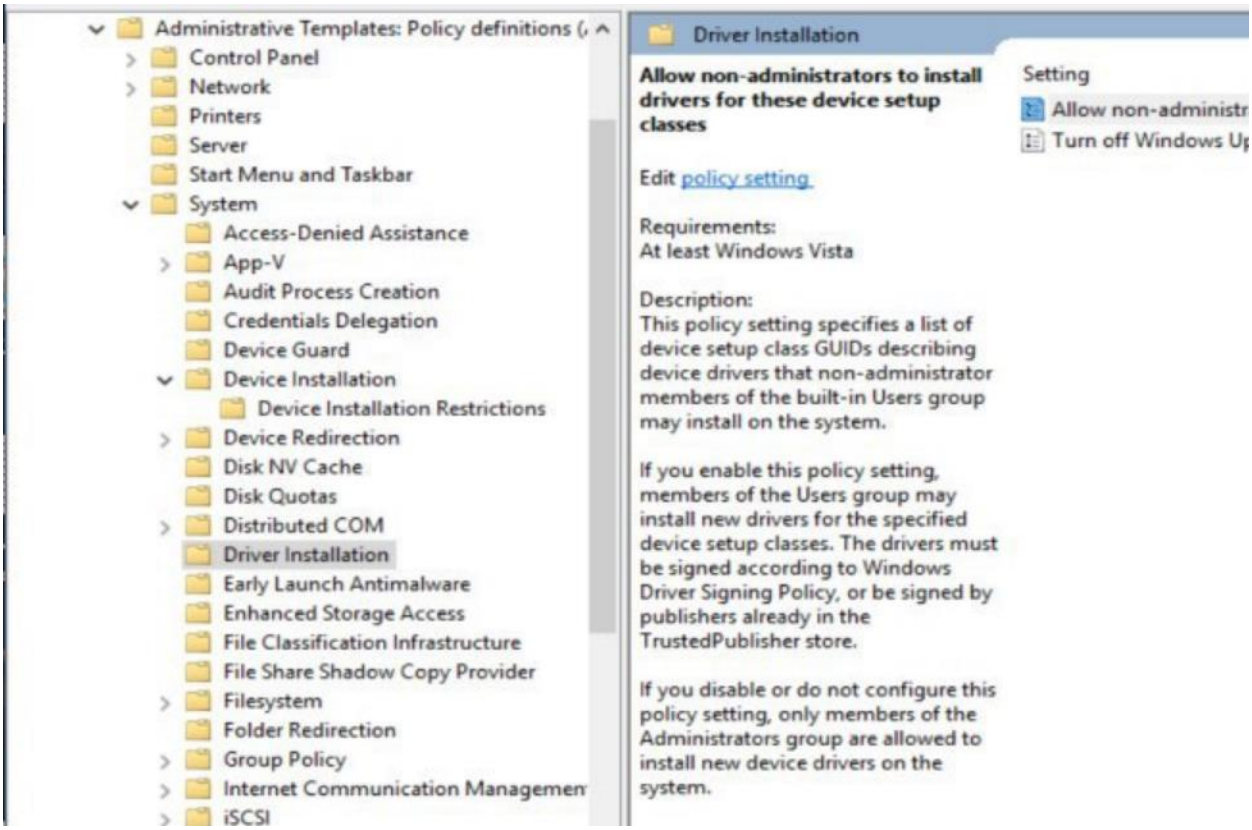

Рисунок 2.11 – Дерево політик у Редакторі групових політик і опис параметру, котрий створює у системі список «безпечних» пристроїв

У цій директорії можна знайти налаштування політики, котре дозволить створити список «безпечних» носіїв інформації. У поєднанні з цим, буде корисно увімкнути параметр політики Prevent installation of devices not described by other policy, котрий знаходиться у другій з перерахованих директорій. Навіть якщо системний адміністратор створив «білий» список знімних носіїв, це налаштування групових політик буде гарантувати, що ніякі інші USB-пристрої не зможуть бути використані в межах існуючої корпоративної мережі.

Проте якщо цей варіант не задовольняє потреби підприємства, можна налаштувати Групові політики таким чином, що в системі буде заборонений запис даних на знімні носії. За це також відповідає певний параметр, котрий можна

знайти в директорії Removable Storage Access. На рис. 2.12 наведений перелік параметрів цієї політики.

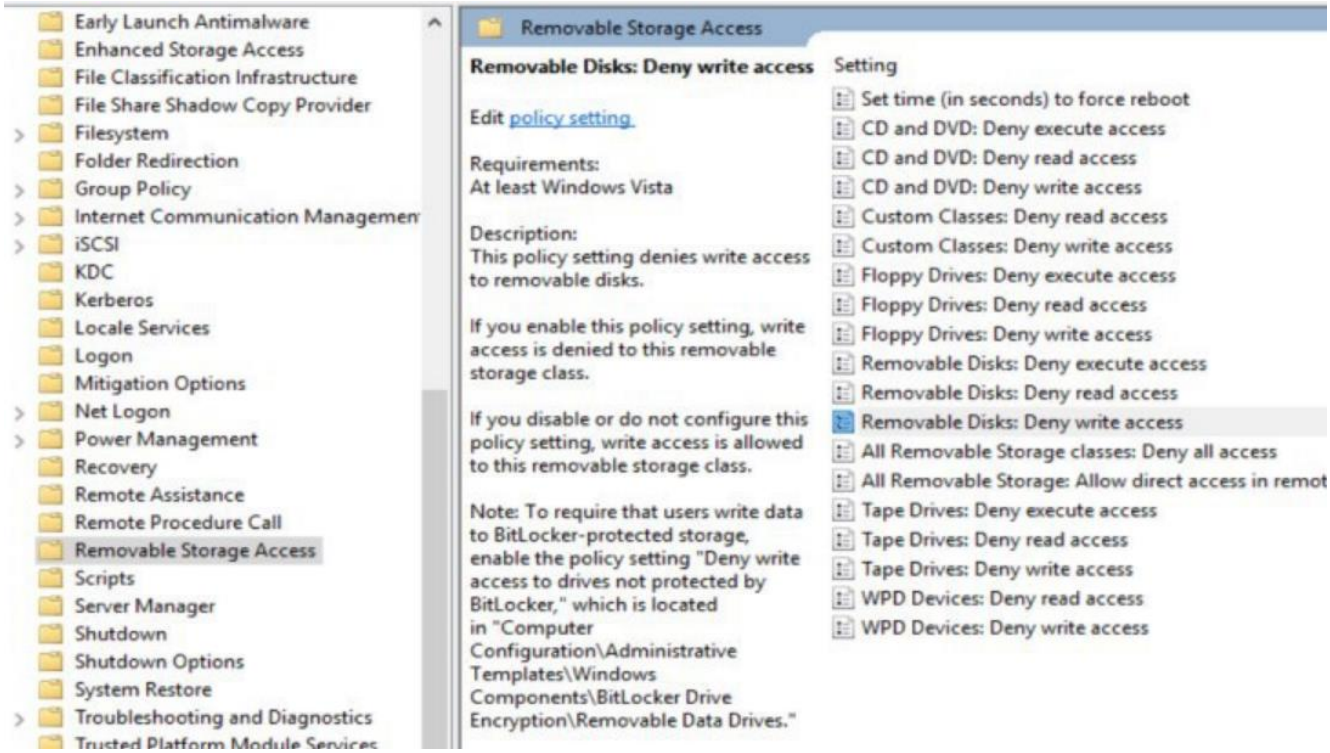

Рисунок 2.12 – Політики доступу до знімних носіїв інформації

У Removable Storage Access знаходиться 19 параметрів, котрі дозволяють встановити дозволи на читання/запис/виконання для різних типів носіїв інформації.

Також, якщо подивитись на рис. 2.12, то можна побачити, що система сама пропонує використати політику обмеження дозволу на запис у поєднані з політикою Bitlocker protected storage.

Взагалі можливості групових політик настільки обсяжні, що системний адміністратор може налаштувати використання функціоналу BitLocker To Go. Таким чином, скопійована на знімний носій інформація буде зберігатися у зашифрованому вигляді і навіть, якщо вона вийде за межі компанії, зловмисник не зможе прочитати збережені дані.

Правильне налаштування групових політик дозволить не тільки контролювати приховані мережі, а й інформацію, що буде мігрувати між різними робочими комп’ютерами підприємства. При чому всі налаштування здійснюються централізовано і приміняються до всіх необхідних членів корпоративної мережі.

Також в залежності від класифікації рівня секретності інформаційних ресурсів, що циркулюють у кожному з організаційних підрозділів, можна створити відповідні налаштування Групових політик. Тобто використання цього функціоналу буде корисним не тільки в контексті прихованих мереж, а й для організації мір інформаційної безпеки у всій корпоративній мережі. Саме цьому буде присвячений наступний розділ атестаційної роботи.

3 ПРОПОЗИЦІЇ ЩОДО ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ГРУПОВИХ ПОЛІТИК ДЛЯ ПРОТИДІЇ ІНСАЙДЕРАМ

Зазвичай корпоративна мережа об’єднує між собою певну кількість комп’ютерів. Чим більша кількість пристроїв підключена до неї, тим складніше системному адміністратору обслуговувати її. Особливо, якщо налаштування робочих машин здійснюється в ручну, то зі збільшенням кількості комп'ютерів, доведеться збільшувати і штат обслуговуючого персоналу. До того ж при великій кількості машин стежити за дотриманням прийнятих на підприємстві стандартів безпеки стає все важче. Групові політики об’єктів (GPO – Group Policy Object) є комплексним інструментом централізованого управління комп'ютерами в домені Active Directory.

Налаштування GPO дозволяє:

- призначати сценарії запуску, входу та виходу в систему;
- поширювати програмне забезпечення в мережі за допомогою публікації або призначення;
- однозначно визначати набір налаштувань безпеки для віддалених елементів мережі;
- визначати політики паролів для облікових записів;
- налаштовувати перенаправлення певних папок з профілю користувача;
- накладати обмеження на робочий стіл;
- визначати налаштування таких категорій, як автономні папки, дискові квоти та ін..

Взагалі ці настройки адміністратор може виконати за допомогою редактора реєстру, але інтуїтивно зрозумілий інтерфейс редактора об'єктів групової політики багато в чому спрощує це завдання.

Об'єкт групової політики – це загальна назва набору файлів, директорій і записів в базі Active Directory (якщо це не локальний об'єкт), які зберігають налаштування системи і визначають, які ще параметри можна контролювати за допомогою групових політик. Створюючи політику, системний адміністратор фактично створює і змінює об'єкт групової політики.

Об'єкти групових політик бувають двох типів: локальний об'єкт групової політики і об'єкти групових політик Active Directory. Локальний об'єкт групової політики може бути тільки один, і це єдиний GPO, який може бути на комп'ютері, що не входить в домен. Він зберігається в SystemRoot/System32/GroupPolicy, а GPO Active Directory зберігаються на контролері домену і можуть бути пов'язані з сайтом, доменом або OU (Organizational Unit, підрозділ або організаційна одиниця). Прив'язка об'єкта визначає його область дії. За замовчуванням в домені створюється два об'єкти групової політики: Default Domain Policy і Default Domain Controller Policy. У першому визначається політика за замовчуванням для паролів і облікових записів в домені, а другий пов'язується з OU Domain Controllers і підвищує настройки безпеки для контролерів домену.

З відпрацюванням Групових політик на певному комп’ютері корпоративної мережі пов’язують наступні етапи обробки даних.

1) Читається реєстр і визначається, до якого сайту належить комп'ютер. Посилається запит серверу DNS з метою отримання IP адрес контролерів домену, розташованих в цьому сайті.

2) Отримавши адреси, комп'ютер з'єднується з контролером домену.

3) Клієнт запитує список об'єктів GP у контролера домену та застосовує їх. Останній надсилає список об'єктів GP в тому порядку, в якому вони повинні застосовуватися.

4) Коли користувач входить в систему, комп'ютер знову запитує список об'єктів GP, які необхідно застосувати до користувача, і застосовує їх.

На 3 етапі клієнт отримує від контролеру домену перелік GPO у тому порядку, в якому вони повинні відпрацювати. Порядок застосування групових політик безпосередньо залежить від їх області дії. Першими застосовуються локальні політики, потім політики, призначені на сайт, потім відпрацьовують доменні політики і потім політики, призначені на OU.

У випадку, коли на певний комп’ютер необхідно примінити конкретне GPO незалежно від інших політик, системний адміністратор може виконати форсування. Тоді обрана політика буде вважатися політикою з найвищим пріоритетом. Це означає, що її параметри не можуть бути перевизначені нижчими політиками, а також на неї не діятиме скасування спадкування.

На наступному – 4 етапі відбувається повторний запит переліку GPO, оскільки будь-який об'єкт групових політик містить два розділи – Computer Configuration і User Configuration, як це показано на рис. 3.1.

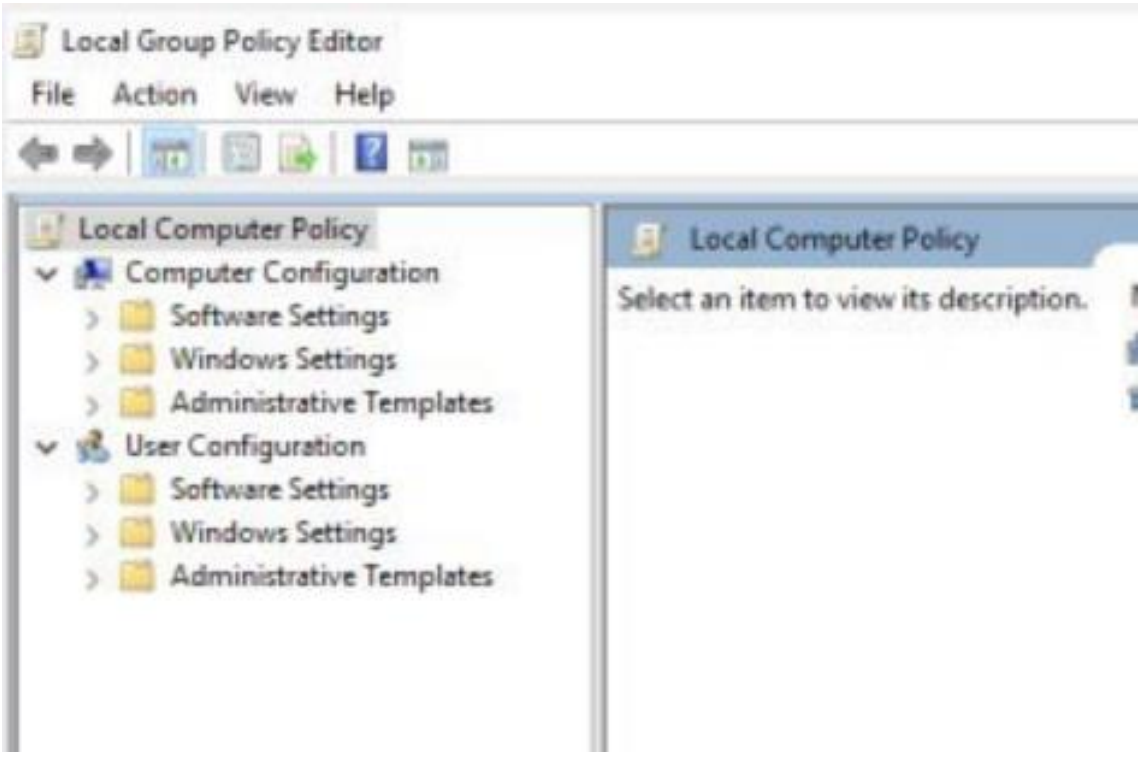

Рисунок 3.1 – Вікно редактору групових політик

Налаштування першого розділу застосовуються під час завантаження Windows і впливають на всіх користувачів даного комп'ютера. Другий розділ містить налаштування облікового запису, які застосовуються під час входу в систему і, відповідно, впливають тільки на цього користувача.

Набір налаштувань для користувача і для комп'ютера досить сильно відрізняється, але все ж можна знайти однакові налаштування, що зустрічаються в обох розділах. І якщо говорити про пріоритет, то політики комп'ютера є більш глобальними і мають більший пріоритет, ніж політики користувача.

Правильне налаштування групових політик дозволить противодіяти витокам інформації з обмеженим доступом через вину штатних працівників. Таким чином, навіть мотивований інсайдер, котрий знає як працює корпоративна мережа, не зможе отримати доступ до конфіденційних даних. Розглянемо більш детально які групові політики можна налаштувати для цього.

3.1 Налаштування політик облікових записів

Якщо перейти у Політики облікових записів у переліку політик першою буде політика Password police. Саме з неї краще почати налаштування групових політик, оскільки парольний захист – це перше, з чим зіштовхується зловмисник при здійсненні атаки. На рис. 3.2 зображені параметри, котрі може налаштувати системний адміністратор.

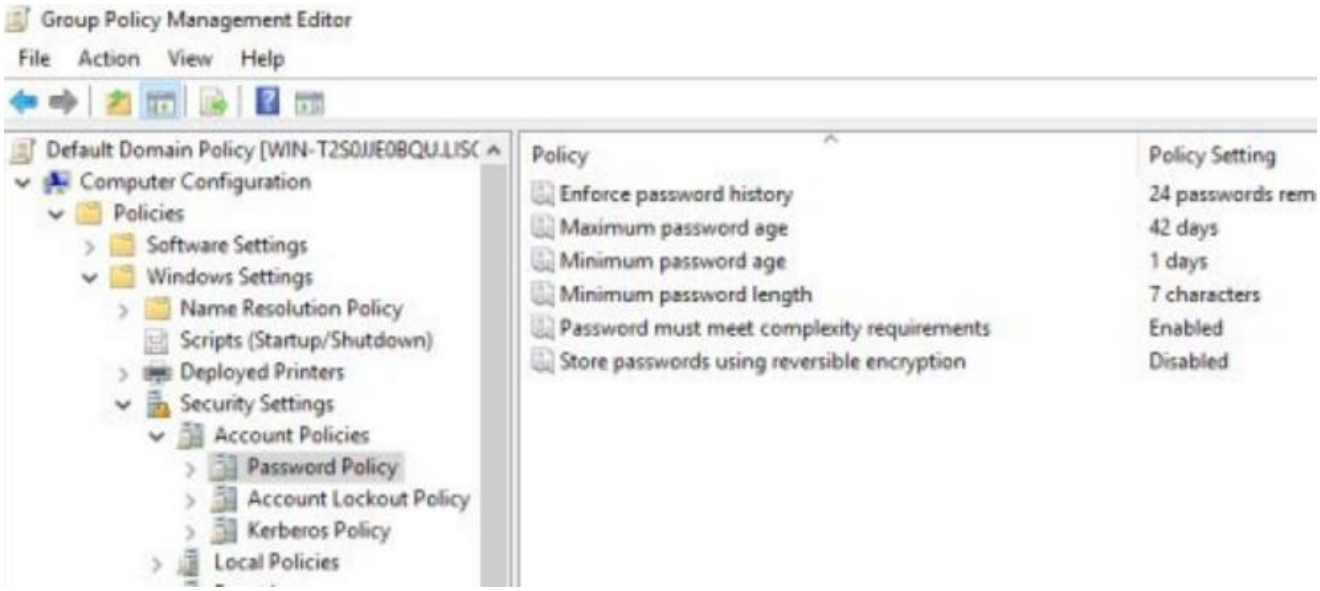

Рисунок 3.2 – Політики паролю, котрі можна конфігурувати відповідно до потреб корпоративної мережі.

Наприклад, перший параметр політики – Enforce password history. Він має значення за замовчуванням для ОС Microsoft Windows Server – 0 паролів, але коли сервер буде приєднаний до домену, то й значення за замовчуванням зміниться на 24 пароля. Ефективність даного параметра політики забезпечується за допомогою параметра Minimum password age, завдяки якому користувачі не можуть змінювати свої паролі занадто часто.

Також необхідно звернути увагу на параметр Password must meet complexity requirements. Він перевіряє всі паролі на відповідність базовим вимогам надійності паролів.

З рис 3.2 видно, що згідно з ієрархією вкладеності наступною політикою є Політика блокування облікових записів. Перелік її параметрів наведений на рис. 3.3.

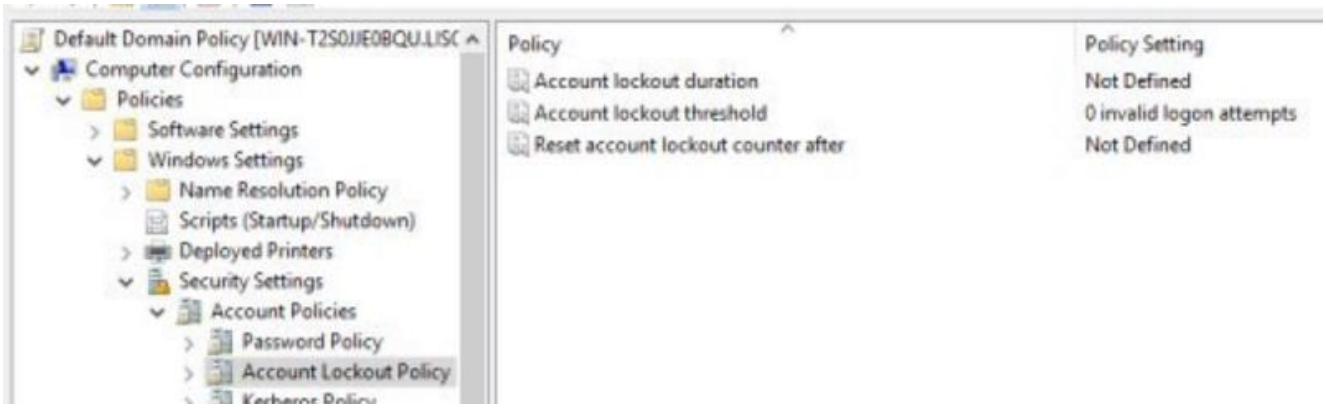

Рисунок 3.3 – Параметри політики блокування облікових засобів

Блокування запобігає входу в корпоративну систему після заданого числа невдалих спроб. Крім того, можна задати тривалість блокування. Внаслідок відпрацювання цієї політики зловмисникам або інсайдерам буде складніше підібрати пароль до облікового запису працівника компанії і таким чином мінімізується ймовірність успіху атак на корпоративну мережу.

Серед зображених на рис. 3.3 параметрів політики, ключовим є Account lockout threshold. Цей параметр політики визначає кількість невдалих спроб входу в систему. Обліковий запис штатного працівника може бути заблокований в результаті помилок при введенні пароля або якщо вводився взагалі невірний пароль. Також можливий варіант, коли користувач змінює свій пароль на одному комп'ютері, а до цього він здійснив вхід на іншому комп'ютері. У такому випадку комп'ютер з невірним паролем буде постійно намагатися аутентифікувати обліковий запис в системі і оскільки при цьому буде використовуватися невірний пароль, відбудеться блокування.

За замовчуванням цей параметр дорівнює 0. Тобто у жодному з випадків не буде відбуватися блокування. Це не правильне рішення з точки зору інформаційної безпеки. Необхідно увімкнути цю політику, проте варто пам’ятати, що зловмисники можуть використовувати стан блокування для атак типу відмова в обслуговуванні (DoS). Для цього їм необхідно буде здійснити блокування великого числа облікових записів.

Тож пропонується декілька варіантів налаштування параметру Account lockout threshold. Для першого варіанту необхідно здійснити наступні налаштування.

1) Задати цьому параметру значення 0, тобто блокування облікових записів буде вимкнуте. Таким чином вдасться запобігти вірогідності виникнення

атак типу DoS. Також у результаті зменшиться кількість звернень до служби технічної підтримки, тому що користувачі не будуть помилково самостійно блокувати свої облікові записи. Проте при цьому залишиться актуальним ризик здійснення успішних атак методом підбору.

2) Обов’язкове використання і конфігурування політики паролів. Користувачі мають використовути складні паролі, що будуть відповідати встановленим у компанії парольним вимогам. Проте встановлений пароль повинен бути таким, щоб робочий персонал мав здатність запам’ятати його, оскільки якщо співробітникам компанії доведеться кудись записувати дані для входу в обліковий запис, то з’явиться ризик розкриття цих даних зловмисниками, а відповідно і ризик отримання доступу до корпоративних ресурсів.

Другий варіант налаштування вказаного параметру політики Блокування облікових записів вимагає наступних дій.

1) Застосувати для параметра Account lockout threshold значення, при якому допускається помилкове введення пароля кілька разів поспіль, але яке забезпечить блокування облікового запису в разі виявлення атаки методом підбору пароля. Такі значення допоможуть запобігти виникненню випадкових блокувань облікових записів працівників. Відповідно зменшиться і кількість звернень до служби технічної підтримки, але в такому випадку буде існувати ризик атак типу DoS.

2) Доповнення мір з першого пункту створенням надійного механізму аудиту, який забезпечить інформування адміністраторів у випадку виникнення одночасних блокувань певної кількості облікових записів. Наприклад, аудит повинен забезпечувати моніторинг подій безпеки під номером 4625. Він представляє невдалу спробу входу в систему, і виявляти, чи був заблокований обліковий запис на момент невдалої спроби входу в систему.

3.2 Налаштування політик призначення прав користувачів

За допомогою політик призначення прав користувача системний адміністратор може визначити, для яких користувачів або груп користувачів будуть надані певні права і привілеї у системі. Всього існує 44 параметри політики Призначення прав користувачів. На рис. 3.4 наведена певна кількість існуючих параметрів. Оперуючи ними, можна обмежити доступ облікових записів

співробітників компанії до певних даних з обмеженим рівнем доступу. Використання даної політики особливо актуально для мінімізації ризиків витоку інформації через деструктивні дії інсайдера. Також чим менше привілеїв має користувач в системі, тим менше вірогідність того, що може статися компрометація даних, наприклад, через халатність штатних працівників компанії.

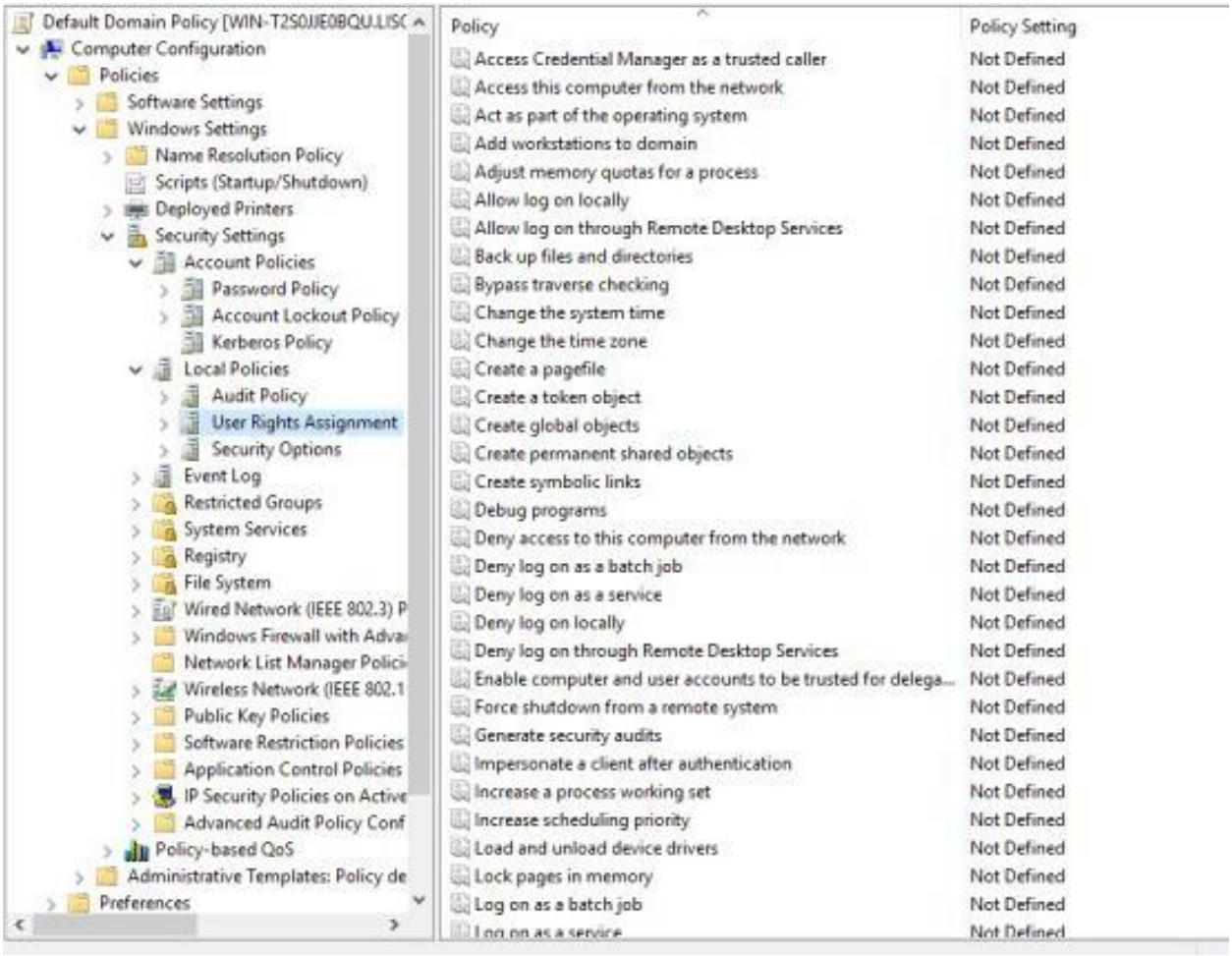

Рисунок 3.4 – Параметри політики Users Rights Assignment

Серед усіх з зазначених на рис. 3.4 параметрів політики Users Rights Assignment необхідно виокремити ряд параметрів, що зможуть підвищити рівень інформаційної безпеки і допоможуть мінімізувати витоки інформації через деструктивні дії інсайдера.

1) Створення маркерного об'єкту. Даний параметр політики дозволяє процесу створювати маркер доступу, який може забезпечувати розширені права доступу до конфіденційної інформації. В системах, в яких безпека має першочергове значення, це право не повинно надаватися нікому з облікових записів користувачів.

2) Заміна маркера рівня процесу. Даний параметр політики дозволяє одному процесу або службі запускати іншу службу або процес з іншим безпечним маркером доступу. Ця можливість може використовуватися зловмисниками для зміни безпечного маркера доступу з метою розширення привілеїв.

3) Відмовити у вході в якості служби. Даний параметр політики визначає, чи можуть користувачі входити як служба. Облікові записи, які мають таку можливість, можуть використовуватися для налаштування і запуску нових неавторизованих служб, таких як кейлогер або інше шкідливе програмне забезпечення.

4) Відхилити локальний вхід. Даний параметр політики забороняє користувачам входити в консоль комп'ютера локально. Якщо неавторизовані користувачі зможуть локально входити в систему, вони отримають можливість завантажувати шкідливий код або розширювати свої права на даному комп'ютері.

5) Створення аудитів безпеки. Цей параметр політики визначає, які користувачі або процеси мають право формувати записи аудиту в журналі безпеки. Зловмисник може використовувати цю можливість для створення великої кількості подій у журналі безпеки. Це ускладнить процес виявлення неправомірних дій для системного адміністратора. Також якщо журнал подій налаштований на перезапис подій у міру необхідності, всі свідчення несанкціонованих дій можуть бути знищені в результаті накладення великої кількості нових подій.

6) Збільшення пріоритету виконання. Даний параметр політики дозволяє користувачам змінювати використаний процесом час процесора. Зловмисник може використовувати цю можливість для підвищення пріоритету процесу до процесу реального часу і, таким чином, створити умову відмови в обслуговуванні (DoS).

7) Відновлення файлів і каталогів. Даний параметр політики визначає, хто з користувачів може обходити дозволи, котрі встановлені для окремих файлів, каталогів, реєстру і інших постійних об'єктів, під час відновлення файлів і каталогів.

8) Зміна власників файлів і інших об'єктів. Даний параметр політики визначає користувачів, які можуть стати власниками файлів, папок, розділів реєстру, процесів або потоків. Це право користувача скасовує всі дозволи, що

застосовуються до захищених об'єктів, і надає право володіння вказаному користувачеві.

Правильне налаштування указаних вище політик дозволить в певній мірі протидіяти витоку конфіденційних даних через вину штатних працівників. Це може стосуватися як і випадкових інцидентів інформаційної безпеки, котрі можуть статися через необізнаність робочого персоналу чи через те, що обліковий запис співробітника мав більше привілеїв, ніж йому потрібно у відповідності до його посади.

Якщо ж говорити, про шляхи пошуку інсайдерів у корпоративних мережах, то вбудовані засоби ОС Windows у поєднані з розгорнутими ролями Active Directory також можуть допомогти налагодити цей процес. Саме тому у наступному розділі будуть розглянуті можливості AD для ідентифікації інсайдерів у корпоративній мережі.

4 ПРОПОЗИЦІЇ ЩОДО ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ВБУДОВАНОГО В WINDOWS SERVER АУДИТУ ДЛЯ ПОШУКУ ІНСАЙДЕРІВ У КОРПОРАТИВНИХ МЕРЕЖАХ

Будь-який адміністратор Active Directory рано чи пізно може зіштовхнутися з необхідністю аудиту корпоративної мережі. Актуальність цієї проблеми пов’язана не лише з ростом структури мережі, а також й зі збільшенням кількості осіб, котрим делеговані права управління в певному сайті або контейнері AD.

Налаштування аудиту дозволяє виділити події безпеки, про виникнення яких будуть інформуватися адміністратори. Події, що були налаштовані для моніторингу, будуть заноситися в спеціальний системний журнал. Цей журнал можна переглянути за допомогою Event Viewer. На рис. 4.1 наведений інтерфейс цього програмного забезпечення.

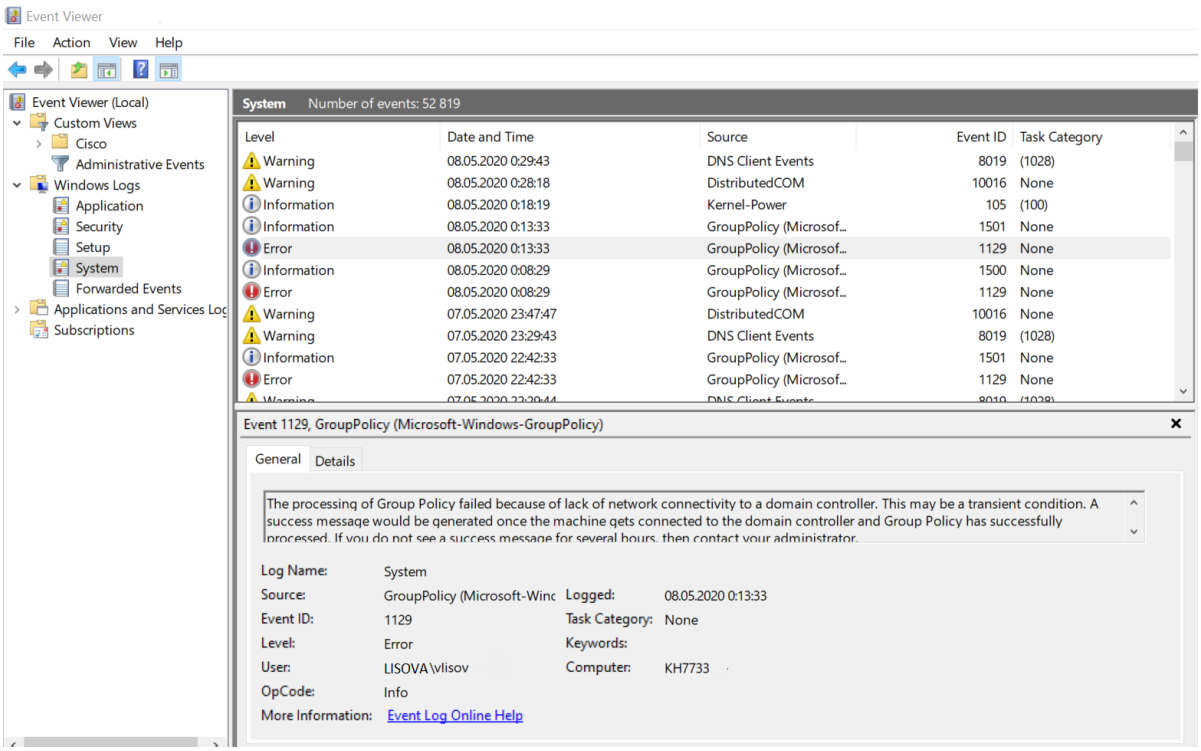

Рисунок 4.1 – Перегляд подій у журналі аудиту за допомогою Event Viewer

Для зручності пошуку і обробки певних подій інформаційної безпеки інтерфейс Event Viewer дозволяє використовувати спеціальні фільтри. Системний адміністратор може відсортувати записи за часом виникнення подій, за рівнем сповіщень (критичне, попередження чи помилка), за кодом події або, якщо вже є

підозра на певного співробітника компанії, за обліковим записом і комп’ютером. В організації може бути велика кількість користувачів, об'єднаних в групи і підрозділи, для яких аудит необхідно налаштувати персонально, але дана можливість в інтерфейсі не передбачена.

Як видно з рис. 4.1 з кожною подією у журналі аудиту пов’язується час виникнення цієї події, джерело та код події. Якщо ж відкрити більш детальну інформацію стосовно певного запису в event.log, то можна знайти інформацію стосовно облікового запису користувача відносно котрого відбулася зафіксована подія. Оскільки інсайдер міг використати чужі облікові дані для того, щоб отримати доступ до конфіденційних ресурсів, системний адміністратор також може визначити і комп’ютер з якого були здійснені маніпуляції. Це допоможе більш детально ідентифікувати місце, в котрому треба шукати інсайдера і, можливо, взагалі знайти цілий підрозділ компанії, в котрому необхідно підвищити рівень інформаційної безпеки.

Також конфігурація політик аудиту дозволить відстежувати події, пов'язані з активністю співпрацівників компанії, наприклад, хто виконує доступ до об'єкта, коли користувачі входять або виходять з системи. Однак перш ніж реалізовувати політику аудиту, слід провести аналіз і вирішити які категорії подій будуть під постійним моніторингом, оскільки відстежувати всі події в системі – це не дуже оптимальний варіант.

По-перше, якщо в журнал подій будуть заноситись усі події, то у разі виникнення інциденту інформаційної безпеки, системному адміністратору буде складно знайти всі пов’язані з подією інформаційні дані.

По-друге, контролер домену може генерувати тисячі подій (наприклад, коли вранці всі працівники приходять на робоче місце і вводять свої облікові дані в систему), а створення такої кількості подій вимагає обчислювальної потужності. Якщо ж системному адміністратору знадобиться здійснювати аудит подібних подій, то потрібно буде збільшити розмір контролера домену, щоб впоратися з навантаженням.

4.1 Робота з журнальними файлами

Правильне налаштування журнального файла дозволить зберігати інформацію про події системної безпеки стільки часу, скільки необхідно для проведення розслідування у разі виникнення інформаційного інциденту. Також це буде корисно, коли в журналах з'являються події, які виглядають підозріло, але в даний проміжок часу ще не можна зробити однозначний висновок стосовно їх впливу на інформаційну безпеку корпоративної мережі. У такому випадку, можна заархівувати цей фрагмент журнально файлу. Таким чином, у разі необхідності до нього можна буде легко отримати доступ і здійснити аналіз зафіксованої інформації.

Щоб створити резервну копію журналу, потрібно натиснути правою кнопкою миші по назві журналу і обрати пункт меню Save All Events As. Процес створення нового архіву відображений на рис. 4.2. За замовчуванням Windows зберігає файл у папці Administrative Tools. Можна вказати іншу папку або створити окрему папку для зберігання архівних копій журналів.

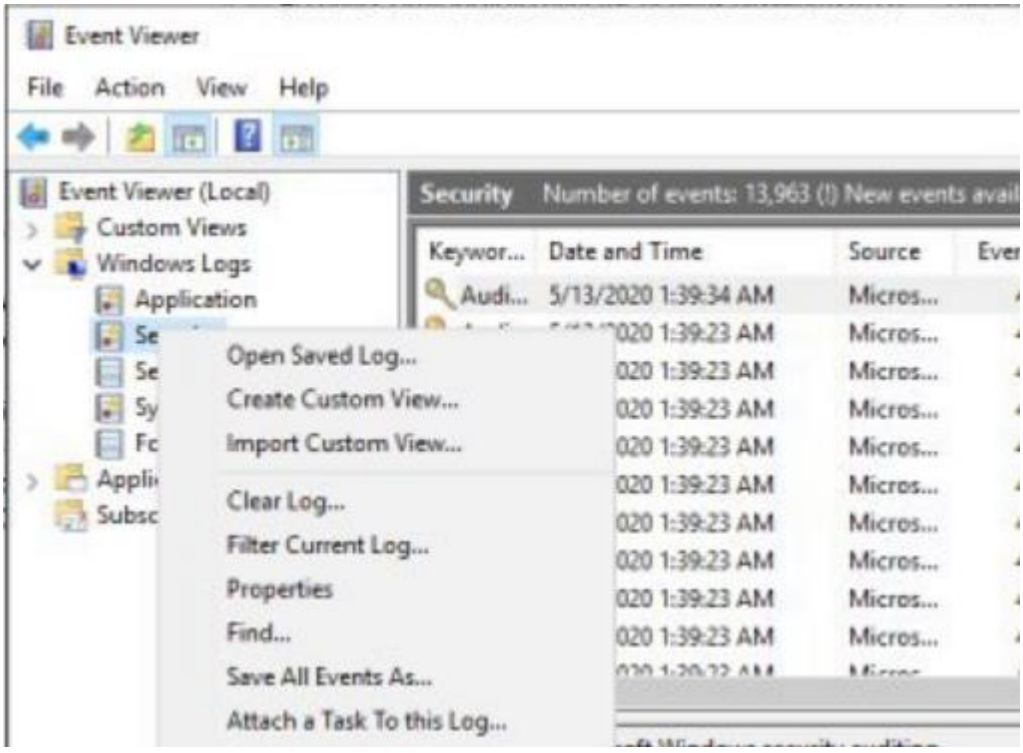

Рисунок 4.2 – Архівування журнального файлу в вікні Event Viewer

Також можна виконати протилежну дію – очистити журнальний файл. Це може бути корисно, коли вже здійснений аналіз зафіксованих подій і серед них не

знайдено повідомлень, які можуть свідчити про виникнення ризику інформаційної безпеки. У результаті буде звільнено додаткове місце для нових записів.

Процес очищення також варто проводити, якщо при конфігуруванні журнального файлу був встановлений параметр Do not overwrite events (clear log manually). На рис. 4.3 зображений цей параметр у вікні Властивостей журнального файлу. У цьому ж вікні можна завдати і максимальний розмір обраного event.log.

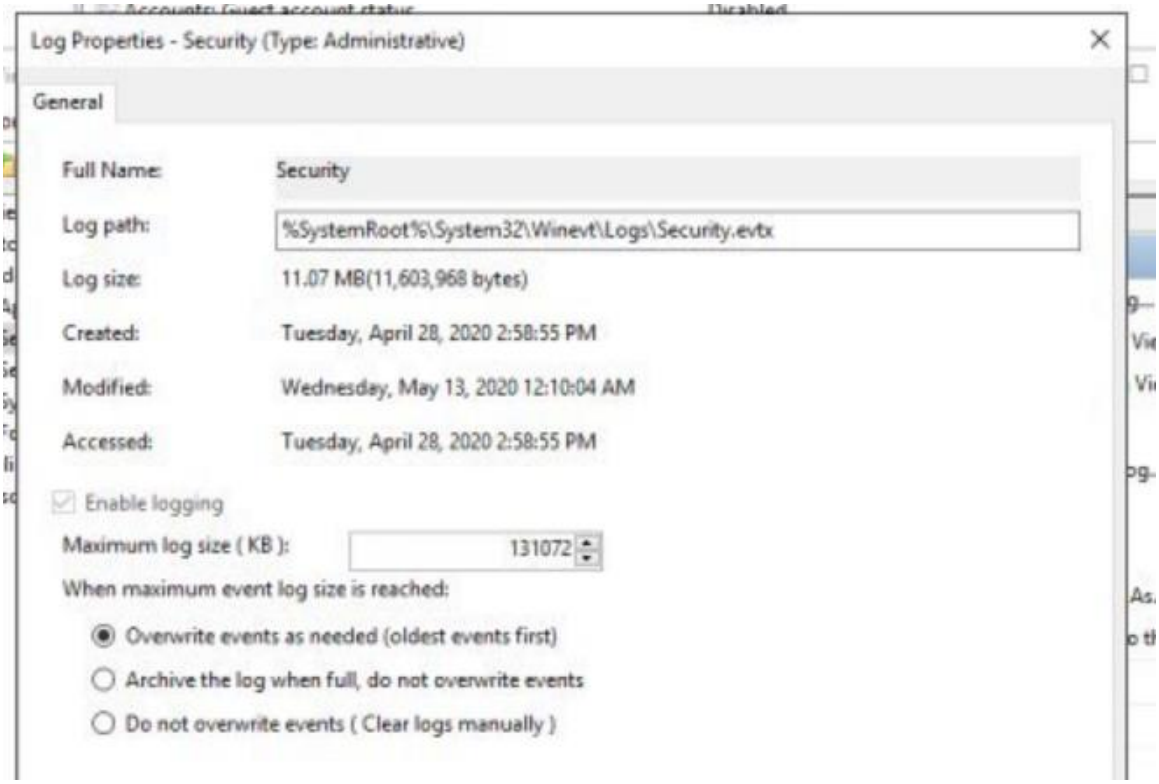

Рисунок 4.3 – Налаштування максимального розміру журнально файлу і вибір процедури, що буде виконуватися після заповнення файлу

Процес очищення журналу запускається натисненням правою кнопкою на назві журналу в списку консолі Event Viewer і вибором пункту Clear Log. Система виведе нове вікно з пропозицією зберегти журнал перед тим, як очистити його. Якщо в журналі є записи, які могли б стати в нагоді в майбутньому (наприклад, при тривалому відстеження проблеми), можна виконати архівацію цього журнального файлу.

Для огляду журналів подій або їх фільтрації в локальних або віддалених комп'ютерах системний адміністратор також може використати PowerShell. Це може бути зручно, коли системний адміністратор одразу знає інформацію

стосовно яких подій він хоче переглянути, або ж його цікавлять загальні дані стосовно існуючих у системі журнальних файлів.

Наприклад, за допомогою команди Get-EventLog можна отримати інформацію стосовно списку всіх журнальних файлів у системі. Також ця команда виведе назву кожного log файлу, його допустимий максимальний розмір і кількість записів у ньому. На рис. 4.4 наведений результат дії цієї команди.

Рисунок 4.4 – Результати роботи команди Get-EventLog

Також за допомогою використання відповідних параметрів можна налаштувати дані, котрі будуть виведені. Наприклад, на рис. 4.5 здійснюється виведення на екран 5 останніх подій в журнальному файлі Directory Service та 5 останніх подій, що відповідають рівню «попередження».

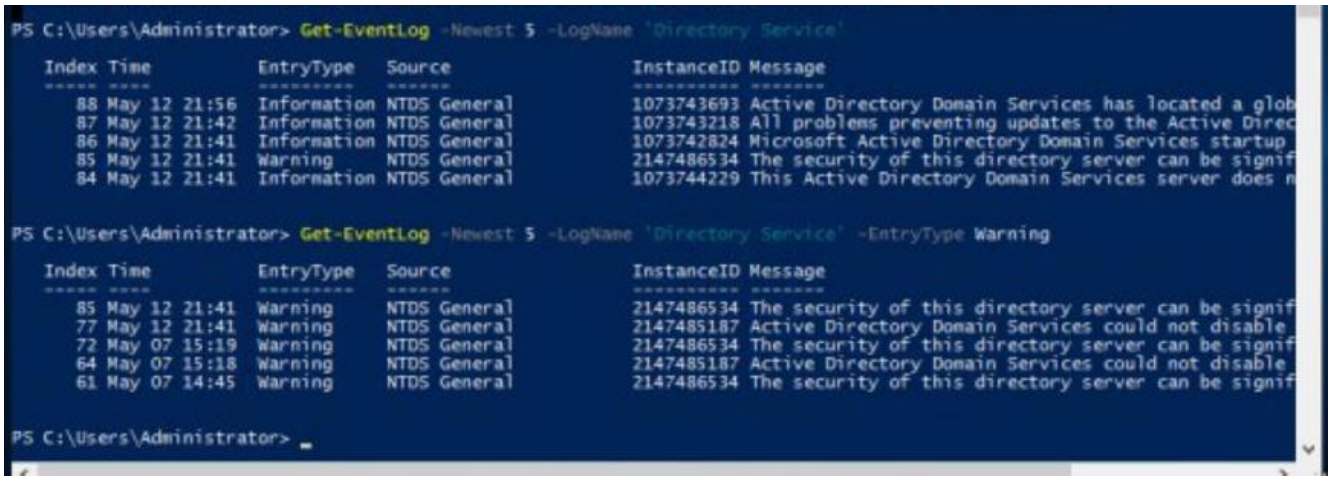

Рисунок 4.5 – Результат роботи команди Get-EventLog з вказаними параметрами

Отже, для дослідження журнальних файлів можна використовувати, як PowerShell, так і графічний інтерфейс Event Viewer. Останній більш зручний у

використанні, хоча використання команд також дозволяє переглянути дані за будь-яким фільтром.

4.2 Налаштування локальних політик аудиту

Для налаштування аудиту подій корпоративної мережі необхідно під’єднатися до контролеру домену і відкрити редактор групових політик. Далі потрібно створити політику в потрібному домені. Взагалі, для включення аудиту можна використати політики домену за замовчуванням, але краще створити окрему політику, так як це спрощує адміністрування. Далі в новій політиці необхідно перейти по ієрархії вкладеностей: Computer Configuratio/Windows Settings/Security Settings/Local Policies/Audit Policy. Після цього системний адміністратор побачить перелік можливих для активування параметрів настройки аудиту. Цей перелік наведений на рис. 4.6.

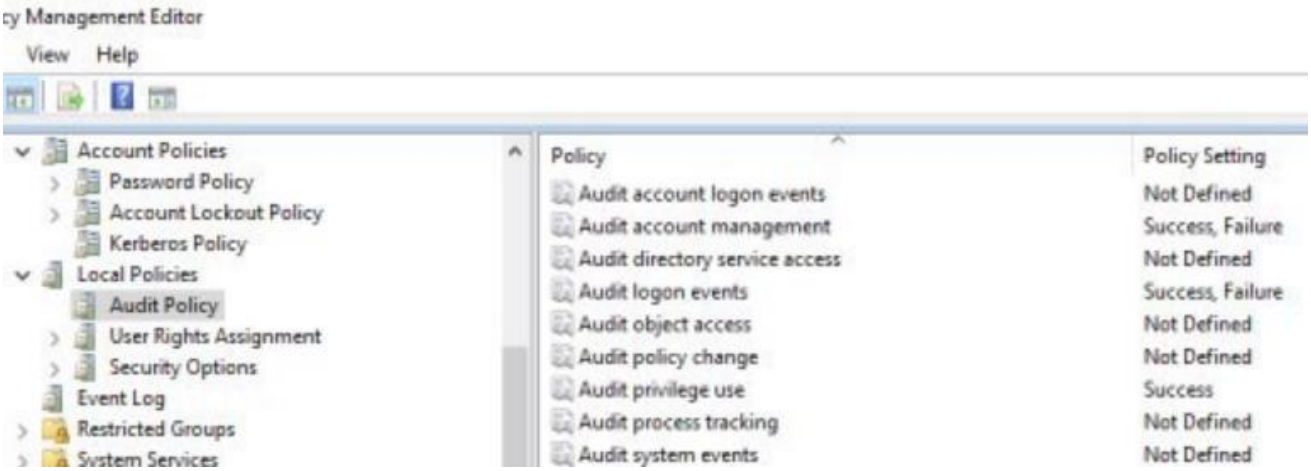

Рисунок 4.6 – Параметри політики аудиту

Проте, як згадувалося вище, не має сенсу налаштовувати аудит на запис усіх подій в системі, оскільки журнал подій швидко наповниться величезною кількістю малоінформативних повідомлень. Це буде заважати здійснювати аналіз активності користувачів в мережі, на основі котрого можна буде зробити висновки про наявність в корпоративній мережі інсайдера. Рекомендовано застосовувати наступний набір значень параметрів політики аудиту, який надано у таблицы 4.1.

Таблиця 4.1 – Рекомендований набір значень параметрів політики аудиту

Назва категорії аудиту	Що буде фіксуватися у журналі
Audit account management	success/failure
Audit directory service access	–
Audit logon events	failure
Audit object access	Вмикається тільки, якщо потрібно відстежувати доступ до певних об'єктів
Audit policy change	success/failure
Audit privilege use	success/failure
Audit process tracking	–
Audit system events	success/failure

Однак, якщо просто налаштувати політики аудиту на кожному з контролерів домену, системному адміністратору буде складно працювати з такою розгалуженою системою. Тому у якості рішення пропонується використання механізму підписки на події. Цей вбудований в Windows Server з розгорнутими ролями Active Directory функціонал дозволяє певній кількості віддалених комп'ютерів пересилати записи про події у системі. Внаслідок цих дій, системний адміністратор зможе централізовано переглянути усі події, що відбулися в корпоративній мережі.

Для того, щоб здійснити підписку на події, необхідно під обліковим записом адміністратора зайти на кожен з серверів і подібно до того, як це робилося у 4 розділі даної атестаційної роботи, активувати служби WinRM. Також необхідно додати до групи локальних адміністраторів сервер, котрий буде виступати у вигляді сховища усіх подій корпоративної мережі.

Після цього необхідно створити саму підписку, за допомогою котрої будуть пересилатися події з журналів. Для цього на центральному сервері необхідно запустити Event Viewer від імені адміністратора, а потім при кліці на Subscription лівою кнопкою миші вибрати пункт меню Create Subscription. Відкриється вікно створення підписки, в котрому необхідно буде ввести ім’я підписки і вказати журнал призначення, до котрого будуть записуватися усі отримані події. За замовчуванням ці події будуть зберігатися в журналі перенаправлених подій в папці Windows Logs.

Також у цьому вікні необхідно буде вибрати усі комп’ютери, від котрих будуть надходити повідомлення про події. Так, на рис. 4.7 зображений процес додавання нового елементу корпоративної мережі до цього переліку.

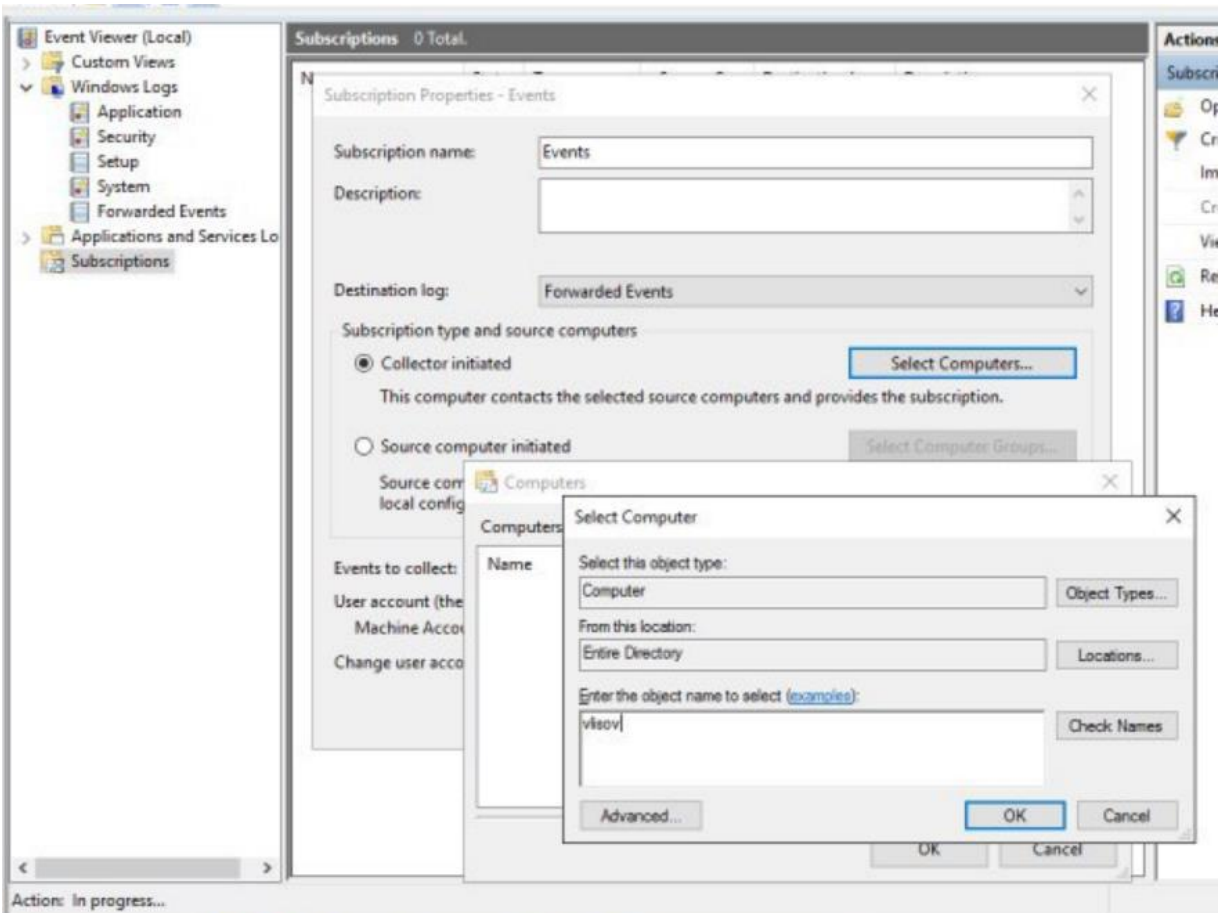

Рисунок 4.7 – Додавання комп’ютеру у список комп’ютерів, від котрих будуть приходи повідомлення про події аудиту

Також у цьому ж вікні можна налаштувати фільтр, котрий буде обробляти отримані дані і зберігати лише ті події, котрі вказав системний адміністратор. Приклад налаштування фільтру наведений на рис. 4.8.

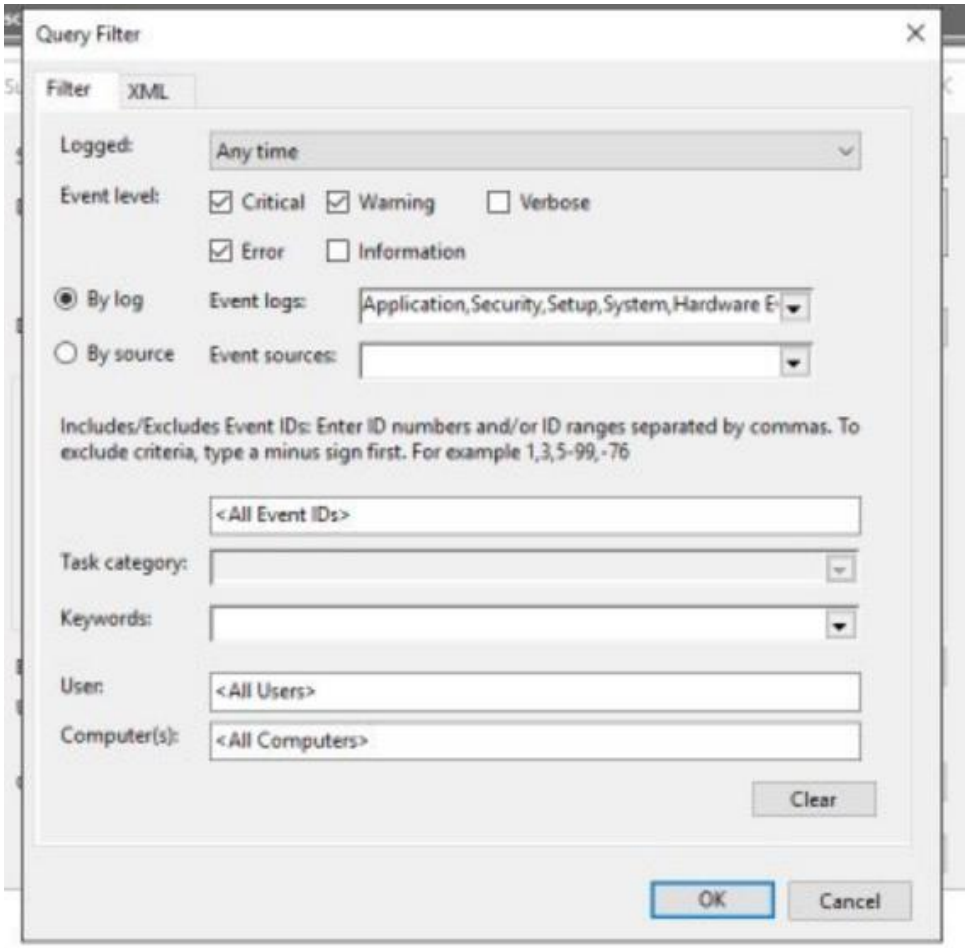

Рисунок 4.8 – Налаштування фільтру подій аудиту

Після цих маніпуляцій системний адміністратор матиме можливість передивлятися усі цікавлячі його події на обраних комп’ютерах корпоративної мережі. На рис. 4.9 наведений приклад відображення подій у журналі аудиту.

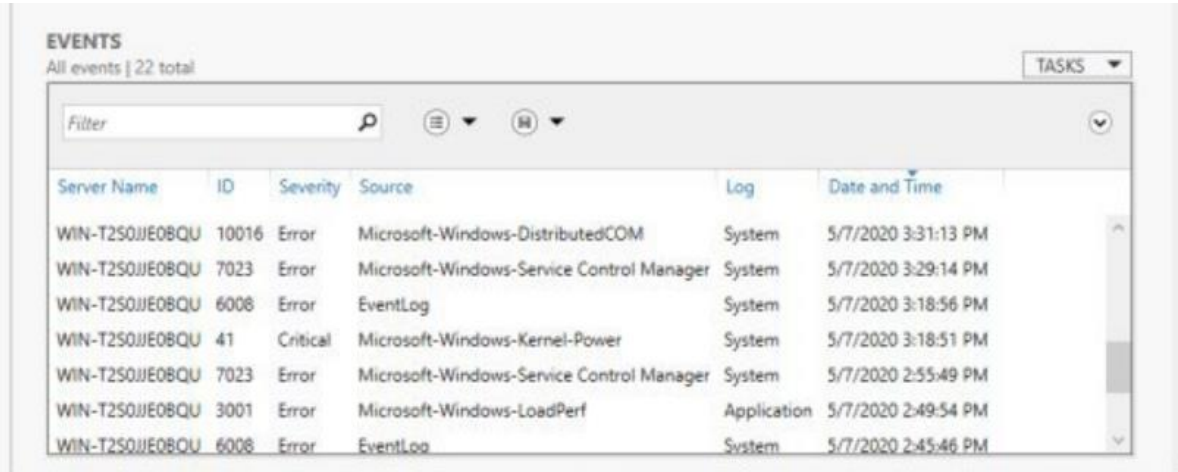

Рисунок 4.9 – Перегляд журналу подій аудиту

4.3 Налаштування розгорнутих політик аудиту

Можливості служб Active Directory також дозволяють налаштувати розгорнуті політики аудиту. Їх варто застосовувати, коли локальних політик аудиту не достатньо. Проте налаштування розгорнутих політик аудиту призведе до того, що будь-яка існуюча раніше політика аудиту перезапишеться, і почне відпрацьовувати щойно встановлена політика. Тому системному адміністратору необхідно точно бути впевненим яку політику він хоче примінити до організаційного підрозділу чи домену.

Також, якщо системний адміністратор вже використав різні групові політики з настройками аудиту, але потреби корпоративної мережі змінились і тепер необхідне використання розширеного аудиту і його під категорій, то для цього випадку Microsoft врахувала і ввела нову політику, яка називається «Audit: Force audit policy subcategory settings to override audit policy category settings». За замовчуванням вона відключена.

На рис. 4.10 у директорії Audit policies наведений перелік політик, котрі можна налаштувати і застосувати. Кожна з політик має перелік параметрів, котрі описують певний тип подій.

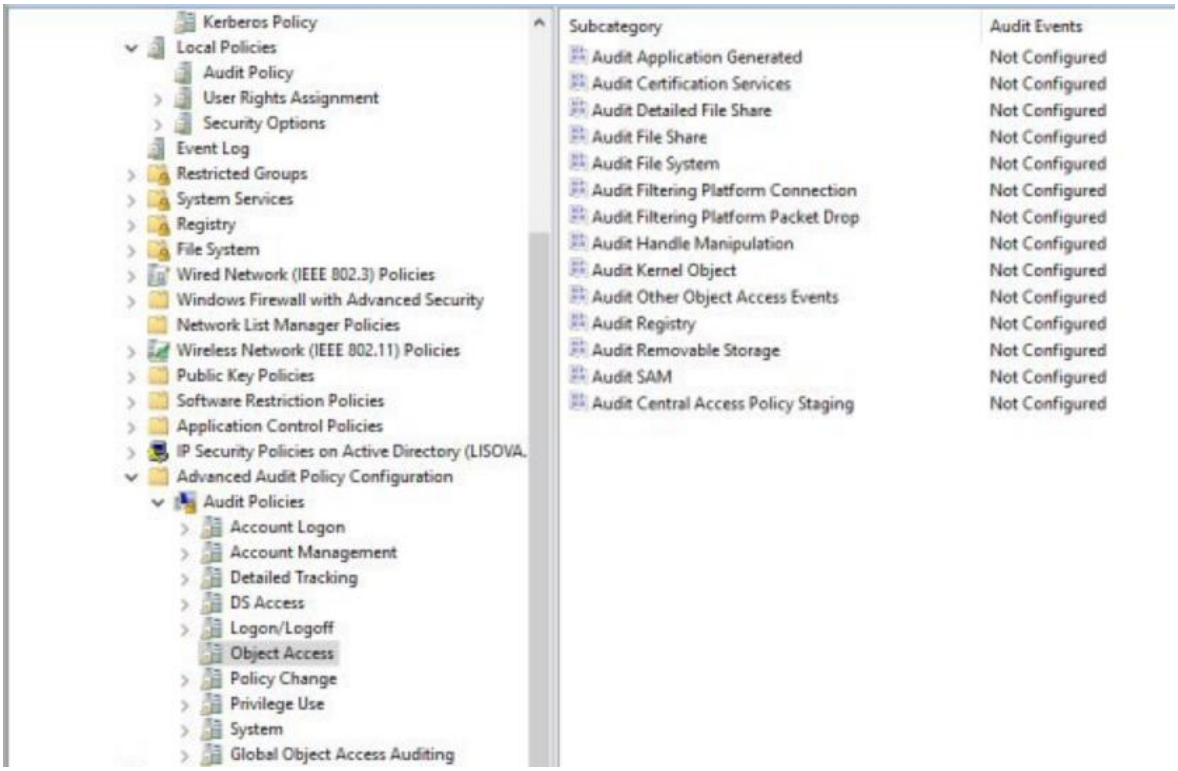

Рисунок 4.10 – Перелік розширених політик аудиту і їх параметри

У контексті пошуку інсайдерів у корпоративній мережі пропонується звернути увагу на параметр політики аудиту Доступ до об'єктів. Параметри цієї категорії визначають необхідність виконання аудиту при доступі користувача до об'єкта-файлу, папки, розділу реєстру або принтеру, для якого визначено системний список управління доступом (SACL).

В файловій системі окрім дозволяючих правил (Allow), існують і забороняючі (Deny). Однак явні заборони зазвичай використовуються досить рідко, оскільки для управління доступом цілком вистачає звичайних дозволів. Більш того, заборони не рекомендується використовувати без крайньої необхідності, оскільки правила заборони завжди мають вищий пріоритет, ніж правила дозволу. Внаслідок цього, при їх використанні можливе виникнення конфліктів доступу. Наприклад, якщо користувач входить в дві групи, в однієї з яких є дозвіл на доступ до папки, а у другій явний заборону, то спрацює заборона і користувачеві буде відмовлено в доступі.

Однак бувають ситуації, в яких застосування заборон може бути виправдане. Наприклад, одному користувачеві необхідно заборонити доступ до папки. При цьому він входить в групу, що має дозволи на доступ. Відібрати доступ у всієї групи не можна, оскільки в неї входять інші користувачі, яким необхідний цей доступ для виконання робочих обов’язків. Прибрати користувача з групи теж не можна, оскільки крім доступу до папки членство у групі налає і інші дозволи, які повинні залишитися. У такій ситуації єдиним виходом залишається тільки явний заборону на доступ для даного користувача. На рис. 4.11 наведений приклад використання правила заборони для користувача vlisov.

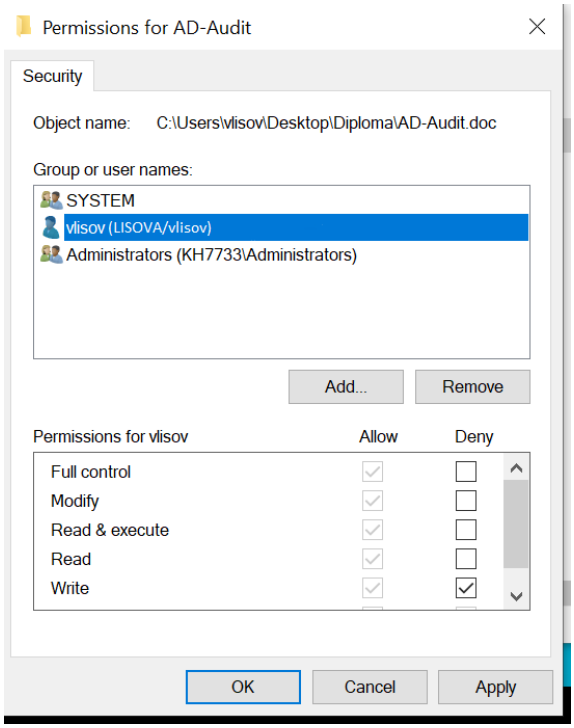

Рисунок 4.11 – Редагування списку SACL для текстового файлу

Таким чином, для користувача vlisov буде заборонено вносити зміни в файл. Це корисно, якщо необхідно захистити конфіденційні дані від підміни. Також у цьому вікні можна заборонити право Modify, і тоді певні користувачі не зможуть не тільки змінити файл, а й відкрити його. У поєднанні з правильно налаштованою політикою аудиту, використання цієї заборони створить в журнальному файлі запис, котрий сигналізуватиме про спробу неправомірного доступу до інформації з обмеженим доступом.

Таким чином, проаналізував запис у event.log системний адміністратор отримає інформацію про те, з якого комп’ютера була здійснена спроба отримати доступ і час. Якщо така подія має одиничний характер, то можна зробити висновок, що користувач міг помилково спробувати відкрити файл, якщо ж у журнальному файлі систематично фіксуються подібні події, то це може свідчити про те, що у корпоративній мережі з’явився інсайдер, котрий свідомо шукає шляхи отримання доступу до конфіденційної інформації.

Отже, при налаштуванні політики аудиту Доступ до об’єктів треба розуміти, що якщо параметру Аудит доступу до об'єктів (Audit object access) буде задано значення Успіх, запис події аудиту буде відображений у журнальному файлі при кожному успішному доступі користувача до об'єкта з заданим SACL. Якщо для

цього параметра політики задано значення Відмова, запис аудиту формується при кожній невдалій спробі доступу користувача до об'єкта із заданим SACL.

Як видно з рис. 4.10 політика аудиту Доступу до об’єктів містить в собі 14 параметрів. Для пошуку інсайдерів у корпоративній мережі пропонується увімкнути наступні:

- аудит файлової системи;
- аудит диспетчеру облікових записів безпеки;
- аудит інших подій доступу до об’єкту.

Наступним етапом у налаштуванні аудиту для пошуку інсайдерів у корпоративній мережі стане конфігурування політики Зміна політики. Ця політика визначає необхідність аудиту будь-якої зміни політик призначення прав користувача, політик брандмауера Windows, політик довіри або змін в самій політиці аудиту і включає в себе 6 параметрів, котрі можна налаштувати відповідно до потреб корпоративної мережі. Для того, щоб зафіксувати дії інсайдера, рекомендовано увімкнути Аудит зміни політики і Аудит зміни політики перевірки справжності. Таким чином, ці параметри дозволять побачити всі привілеї облікового запису, які зловмисник намагається підвищити. Наприклад, якби зловмисник спробував вимкнути аудит, ця подія була б зареєстрована у журнальному файлі.

Також необхідно звернути увагу на конфігурування політики Облікових записів. Ця категорія аудиту допомагає відслідковувати спроби:

- створення нових користувачів або груп;
- зміни імен користувачів або груп;
- активації або деактивації облікових записів користувачів;
- зміни паролів облікових записів;
- активації аудиту подій управління обліковими записами.

Якщо правильно відконфігурувати цю політику аудиту, системні адміністратори зможуть відстежувати події виявлення зловмисних, випадкових і авторизованих спроб створення облікових записів користувачів або груп. Це несе загрозу для конфіденційних даних, оскільки, наприклад, мотивований або ображений інсайдер, котрий має адміністративні привілеї у системі, може створити або змінити певні налаштування у системі і надати доступ до захищених даних третій особі, що приведе до виникнення інциденту інформаційної безпеки.

Для пошуку інсайдерів у корпоративній мережі і виявлення спроб отримання доступу до ресурсів з обмеженим доступом, рекомендується налаштувати наступні політики аудиту: Управління обліковими записами, Управління обліковим записом комп'ютера, Управління групою безпеки.

Також для максимальної продуктивності аудиту системи, необхідно виконати ще одне налаштування – увімкнути повне логування роботи найпотужнішого інструменту ОС Windows – PowerShell [10]. Після конфігурування цієї політики PowerShell буде реєструвати в журналі події з кодом 4104. У детальній інформації до цих подій буде виводитися інформація щодо запущених блоків сценаріїв, тобто – шлях, тіло скрипта і всі використовувані командлети. Це відображено на рис. 4.12.

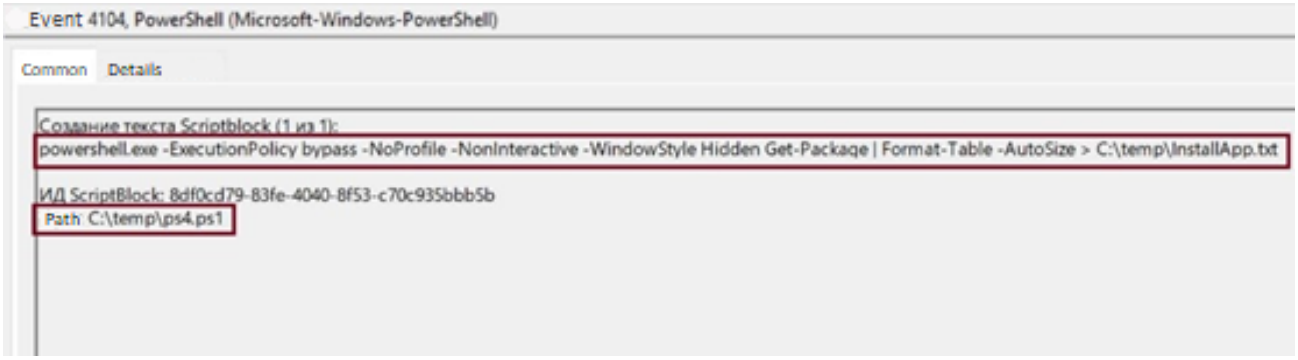

Рисунок 4.12 – Інформація стосовно події з кодом 4104

На основі отриманих даних також можна зробити висновки стосовно того, яким чином виник витік конфіденційної інформації, яке шкідливе програмне забезпечення відпрацювало на робочій станції і які команди для цього були введені. Також системний адміністратор може переглянути коли і ким всі ці події здійснювалися.

Для увімкнення реєстрації блоків сценаріїв командної оболонки PowerShell необхідно налаштувати політику, що знаходиться за наступним шляхом вкладеностей – Administrative Templates/Windows Components/Windows PowerShell. Далі необхідно відшукати параметр Turn on PowerShell Script Block Logging і зробити його активним. Фрагмент цього процесу наведений на рис. 4.13.

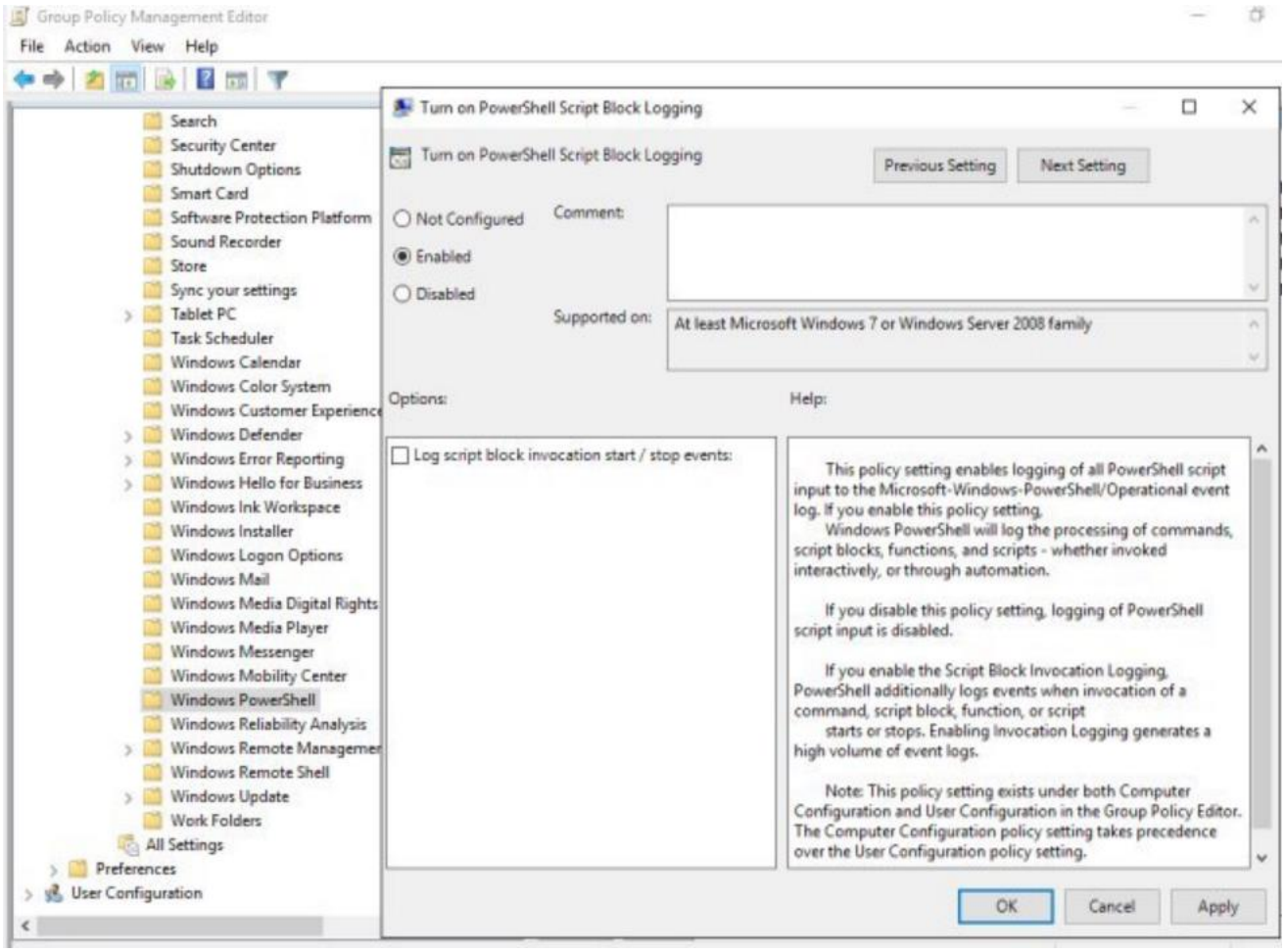

Рисунок 4.13 – Налаштування параметру Turn on PowerShell Script Block Logging

Також, аналогічно до увімкнення аудиту командної оболонки PowerShell, можна налаштувати аудит командної оболонки cmd.exe. Для цього необхідно прослідкувати наступним шляхом: Computer Configuration/Administrative Templates/System/Audit Process Creation, а потім застосувати параметр Include command line in process creation events.

Після налаштування Політики командного рядка в журналі подій Security для події з кодом 4688 з'явиться додаткове значення «Командний рядок процесу» (Process Command Line). У цьому полі буде фіксуватися тіло команди, котру міг застосувати зловмисник. Наприклад, на рис. 4.14 відображений результат включення цієї політики.

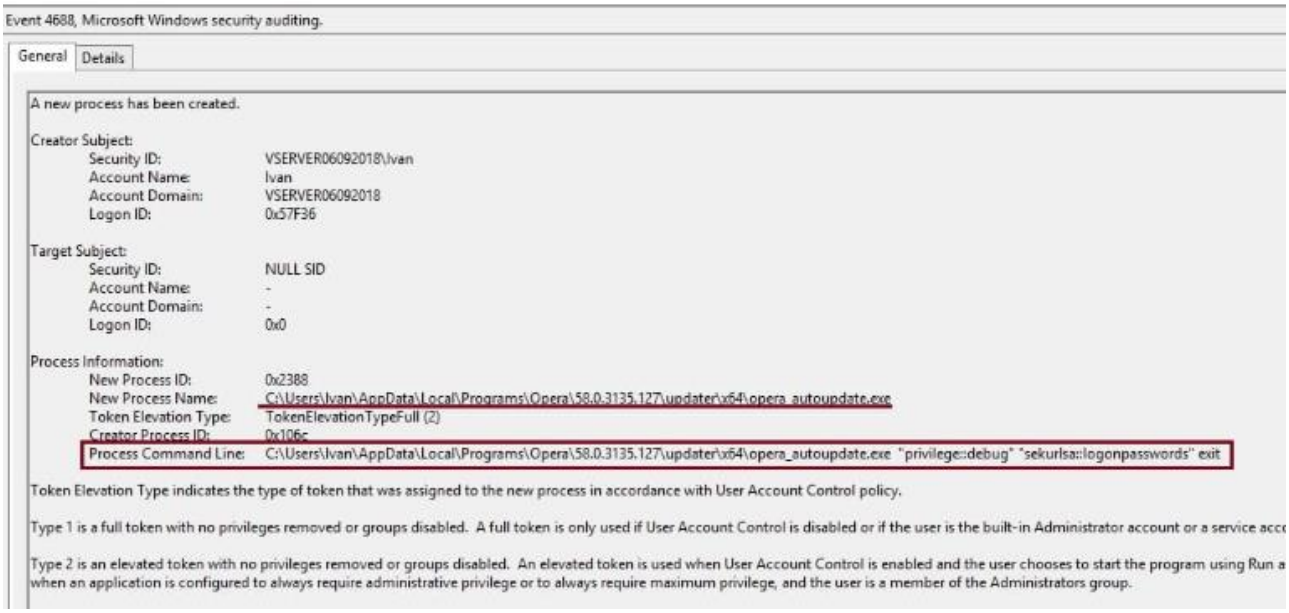

Рисунок 4.14 – Перегляд події 4688 після увімкнення аудиту командного рядка

Якщо подивитися на рис. 4.14, то на перший погляд цей запис у журнальному файлі свідчить про те, що відбувається запуск легітимного процесу «opera_autoupdate.exe». Проте поле «Process Command Line» свідчить про те, що була запущена утиліта «mimikatz». Це не вдалося б зафіксувати без активованого аудиту командного рядка.

Відомо, що Mimikatz – інструмент, який реалізує функціонал Windows Credentials Editor. Тобто, якщо зловмисник запустить цю утиліту на комп'ютері будь-якого зі співробітників компанії, то йому вдасться отримати у відкритому вигляді дані облікових записів користувачів. Це може нанести величезних збитків компанії. Особливо, якщо буде отриманий доступ до облікових записів користувачів з широким спектром привілеїв у системі. Чим більше дозволів матиме скомпрометований акаунт користувача, тим більше конфіденційних даних може розкритися.

Звичайному зловмиснику буде складно підібратися до командного рядка і ввести команду, оскільки необхідно подолати парольний захист. Проте, якщо у компанії розповсюджена практика, коли одним комп'ютером користується декілька людей з різними обліковими записами, то це може нести велику загрозу. Оскільки якщо один зі співробітників виявиться інсайдером, то йому нічого не завадить ввести потрібну команду і запустити шкідливу утиліту.

Налаштування і використання усіх описаних у цьому розділі політик аудиту дозволить створити точний і зручний механізм пошуку інсайдерів у

корпоративних мережах. При виникненні інциденту інформаційної безпеки, системному адміністратору необхідно буде відслідкувати останні події у журнальному файлі і на основі отриманої інформації зробити висновки стосовно активності інсайдерів у мережі.

4.4 Підсилення механізмів виявлення інсайдерів у корпоративній мереж за допомогою використання Advanced Thread Analytics

Для пошуку інсайдерів у корпоративній мережі пропонується використання Advanced Threat Analytics (ATA). Це локальна платформа, розроблена компанією Microsoft, котра спрямована на організацію захисту інформаційних систем від кібератак та шкідливої діяльності інсайдерів.

Впроваджений у корпоративну мережу Advanced Threat Analytics починає вивчати поведінку користувачів. При наявності підозрілої активності цей інструмент може відзначати незвичайні події та видавати попередження на веб-консоль, використовуючи інтерфейс у вигляді стрічки повідомлень. Додатково, якщо потрібно, ATA відсилає попередження по електронній пошті.

Системний адміністратор може налаштувати в Advanced Threat Analytics відправку електронних листів конкретним користувачам або групам в організації при виявленні підозрілої активності. У кожен лист буде включене посилання на конкретну атаку у часовій шкалі атак ATA. Це своєчасно інформує уповноважених осіб про проблеми, пов'язані з безпекою, навіть коли вони не відслідковують тимчасову шкалу атак.

Продукт інтегрується з системами класу Security Information and Event Management (SIEM) за допомогою збору даних і складання звітів. ATA не встановлюється на контролери домену в середовищі. Замість цього використовується віддзеркалення портів для відсилання трафіку контролерів домену на шлюз ATA, де він обробляється. Якщо у корпоративній мережі використовуються віртуальні контролери домену, тоді можна задіяти віддзеркалення портів. У випадку використання фізичних контролерів домену, системному адміністратору необхідно буде налаштувати спеціальне мережеве обладнання для віддзеркалення трафіку. Після успішного налаштування віддзеркалення, Advanced Threat Analytics починає аналізувати дані, взаємодіючі з

контролерами домену та системами SIEM. Потім усі дані передаються на центральний сервер ATA Center, який виконує глибокий аналіз.

Також для розслідування інцидентів інформаційної безпеки буде зручно досліджувати схему забезпечення безпеки в організації, котра представляє собою карту взаємодії об'єктів, на котрій фіксується не тільки контекст дій, а й самі дії користувачів, пристроїв і ресурсів.

Інтерфейс Advanced Threat Analytics підтримує мобільні пристрої, а це значить, що де б не знаходилися ресурси підприємства: в межах організації, на мобільних пристроях або в інших місцях – ATA проводить їх автентифікацію і авторизацію. Тобто зовнішні ресурси, такі як пристрої і постачальники, відслідковуються настільки ж ретельно, як і внутрішні ресурси

Технологія ATA виявляє безліч підозрілих дій, зосередивши увагу на декількох етапах ланцюжка знищення кібератак, включаючи:

– розвідку, в ході якої зловмисники збирають інформацію про те, яку структуру має корпоративна мережа, які інформаційні активи і які об'єкти існують (як правило, саме тут зловмисники будують плани для своїх наступних фаз атаки).

– бічний цикл руху, протягом якого зловмисник вкладає час і зусилля в поширення своєї атаки всередині вашої мережі.

– доменна сталість, під час дослідження якої зловмисник збирає інформацію, яка дозволяє йому провести свою атаку, використовуючи різні набори точок входу, облікових даних і методів.

Ці етапи кібератак завжди мають схожий характер і можуть бути передбачені, незалежно від того, яка організація піддається атаці або на яку інформацію націлена атака. ATA здійснює пошук трьох основних типів атак: зловмисні атаки, ненормальна поведінка і проблеми безпеки і ризики.

Advanced Threads Analytics виявляє ці підозрілі дії і відображає інформацію в консолі ATA, даючи можливість створити чітке уявляння про те хто, що і коли здійснив. Наприклад, на рис. 4.15 представлене попередження про те, що ATA підозрює, що була зроблена атака Pass-the-Ticket на комп'ютерах клієнта 1 і 2.

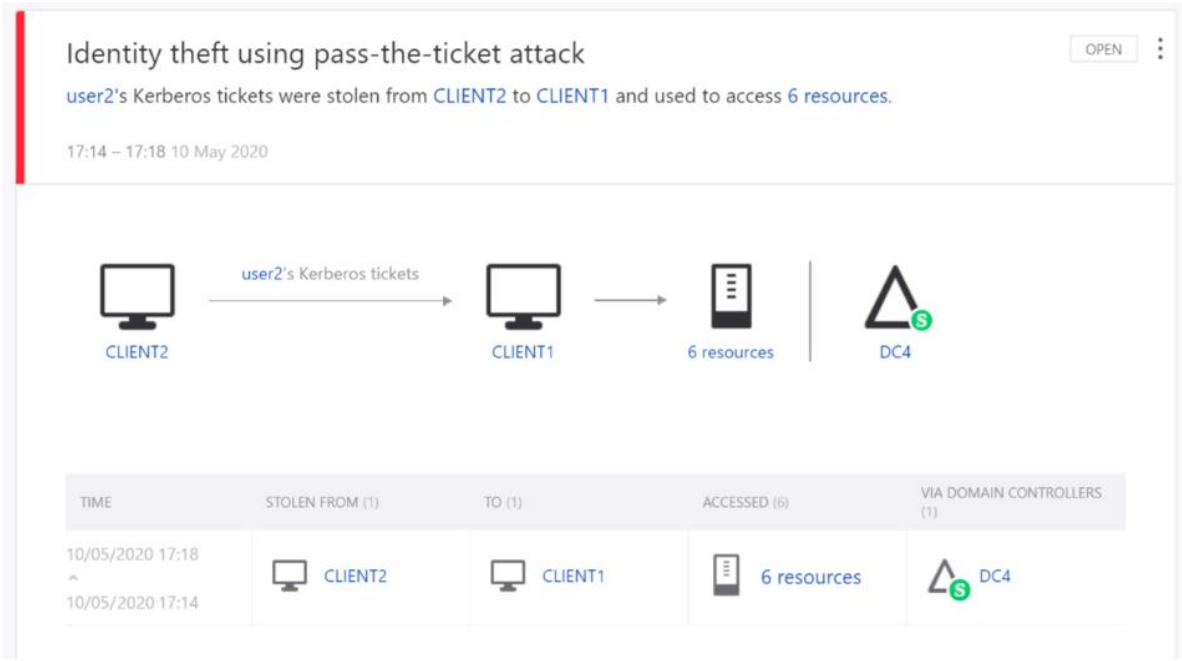

Рисунок 4.15 – Попередження про підозру здійснення атаки Pass-the-Ticket на комп’ютери корпоративної мережі

Також інтерфейс ATA допомагає виявити ненормальну поведінку у мережі, використовуючи поведінкову аналітику і машинне навчання для виявлення сумнівних дій і підозрілої поведінки користувачів та пристроїв у мережі. За допомогою Advanced Threads Analytics можна зафіксувати:

- аномальні логіни;
- невідомі загрози;
- обмін паролями;
- модифікацію чутливих груп.

На рис. 4.16 наведений приклад того, як програмний інтерфейс ATA попереджає системного адміністратора, про факт пересилання даних між чотирма комп'ютерами, до яких цей користувач зазвичай не звертається. Це може стати причиною тривоги, оскільки обліковим запис може використати зловмисник або інсайдер, щоб отримати доступ до конфіденційних ресурсів компанії.

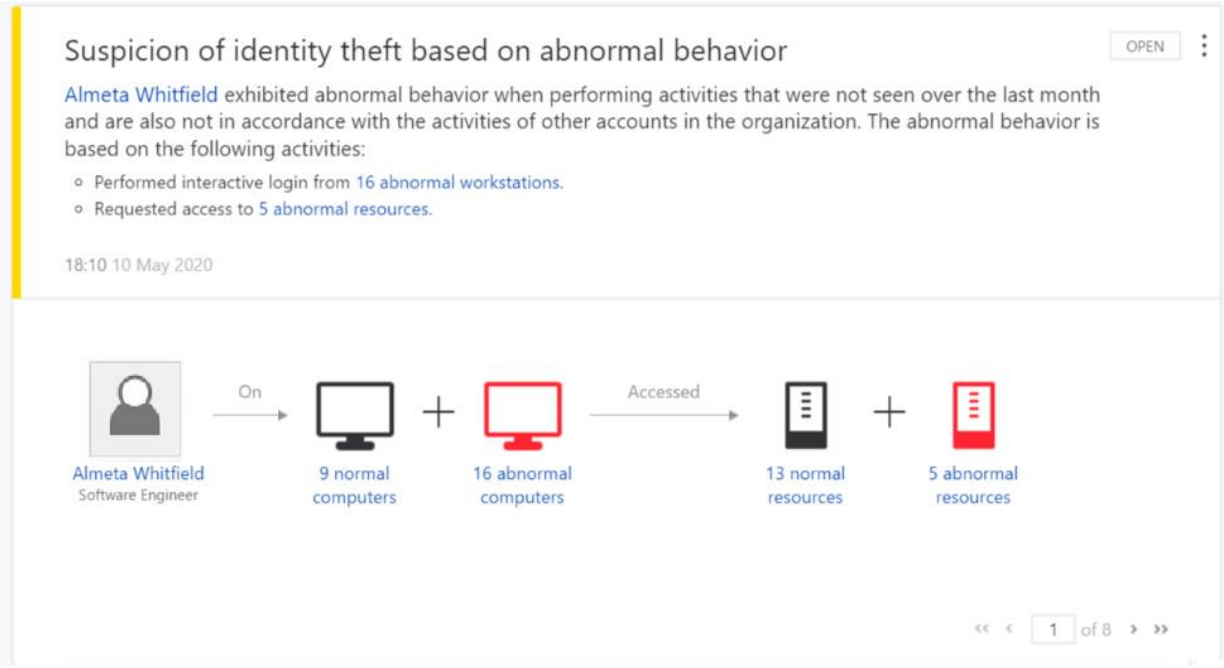

Рисунок 4.16 – Попередження про аномальну поведінку у корпоративній мережі

Якщо порівнювати Advanced Thread Analytics з використання політик аудиту, то можна виокремити ряд переваг.

1) Мінімум налаштувань: ATA має необхідний вбудований інтелект безпеки. Отже немає потреби для настройки правил або політик щодо виявлення загроз безпеки. Настройка ATA досить проста і цей програмний інтерфейс потребує мінімальної подальшої підтримки.

2) Прості повідомлення: при використанні ATA більше немає додаткових звітів і журналів для аналізу. Система сама по собі виконує весь аналіз відомостей і інформує системного адміністратора про критичні повідомлення. Вона здійснює це або у вигляді повідомлень електронної пошти, або у вигляді відображення тимчасової лінії атак через свій веб інтерфейс.

3) Оновлення бази загроз, що дозволяє своєчасно виявити нові проблеми безпеки в інфраструктурі в міру їх виникнення.

4) Підтримка мобільності: Advanced Thread Analytics здатна моніторити події як користувачів з внутрішнього середовища, так і зовнішнього (співробітники, що працюють віддалено); якщо налаштована автентифікація і авторизація, інтерфейс трактує всі підключення як рівнозначні. Тобто не потрібно вносити зміни в настройках, щоб відстежувати підключення із зовнішніх мережевих середовищ.

Використовуючи власний пропріетарний алгоритм, Microsoft Advanced Threat Analytics допомагає цілодобово виявляти підозрілі дії в системах за допомогою профілювання і завдяки знанню того, що шукати. Системному адміністратору не потрібно буде створювати правила, точно налаштовувати систему або відслідковувати потік звітів від системи безпеки, оскільки вся необхідна аналітика вже вбудована.

ВИСНОВКИ

Завдання на атестаційну роботу виконано у повному обсязі. В атестаційній роботі досліджені способи пошуку інсайдерів у корпоративних мережах за допомогою використання механізмів серверних операційних систем, та запропоновано використання механізму захисту від інсайдерських атак.

З цією метою був проведений аналіз каналів витоку інформації внаслідок деструктивних дій інсайдерів. Було встановлено, що найбільша частка витоків припадає на мережевий канал. Виявлено, що найбільш актуальною проблема розкриття даних через вину штатних співробітників є для корпоративних мереж з контролером домену і розгорнутими ролями Active Directory. Встановлено, що внаслідок дій інсайдерів можуть виникати приховані мережі. Були запропоновані методи пошуку прихованих мереж і способи захисту конфіденційних даних в них.

Також було встановлено, що використання штатних засобів операційної системи є більш надійним варіантом, оскільки це відкидає можливість відпрацювання шкідливого програмного коду у корпоративній мережі. Саме тому задача пошуку інсайдерів в корпоративній мережі була вирішена і реалізована на основі налаштувань системи аудиту подій. У ході конфігурування аудиту був досліджений журнал подій.

Результати роботи можуть бути корисні для спеціалістів в області інформаційної безпеки, а також при розробці та функціонуванні систем менеджменту інформаційної безпеки.

Окремі результати роботи доповідались на XLIII Міжнародній науково-практичній інтернет-конференції «Сучасні виклики та проблеми науки» [1 – 3], на Всеукраїнської науково-практичній конференції здобувачів вищої освіти й молодих учених [4], а також на XXII Міжнародному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті» [5].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Лісова В. П. Пропозиції щодо побудови корпоративних мереж [Електронний ресурс] / В. П. Лісова // Матеріали XLIII Міжнародної науково-практичної інтернет-конференції «Сучасні виклики та проблеми науки». – 2020 – Ч. 3, С. 11.

2. Лісова В.П. Пропозиції щодо використання служби Active Directory щодо виявлення прихованих мереж [Електронний ресурс] / В.П. Лісова // Матеріали XLIII Міжнародної науково-практичної інтернет-конференції «Сучасні виклики та проблеми науки». – 2020. – Ч. 3, С. 17.

3. Lisova V.P., Podoliaka N.V. Suggestions of protection confidential data from insider attacks / V.P. Lisova, N.V. Podoliaka // Матеріали XLIII міжнародної науково-практичної інтернет – конференції «Сучасні виклики та проблеми науки». – 2020. – Ч. 3, С. 23.

4. Лісова В.П. Аналіз методів пошуку прихованих мереж в корпоративній мережі з розгорнутими ролями Active Directory / В.П. Лісова, І.С. Добринін // Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених, листопад 2018 року, м. Кропивницький, Кропивницький ЦНТУ. – Кропивницький ЦНТУ, 2018, 411 с.

5. Лісова В.П. Пропозиції щодо використання служби Active Directory щодо виявлення прихованих мереж / В.П. Лісова, І.С. Добринін // Матеріали 22-го Міжнародного молодіжного форуму "Радіоелектроніка і молодь в XXI столітті", березень 2018 року, м. Харків, ХНУРЕ. - Харків: редакційно-видавничий відділ ХНУРЕ, 2018, 222 с.

6. Глобальне дослідження витоків конфіденційної інформації у перше півріччя 2019 року [Електронний ресурс]. – Режим доступу до ресурсу: https://www.infowatch.ru/analytics/reports/17376

7. Як захистится від інсайдера [Електронний ресурс]. – Режим доступу до ресурсу: http://www.iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov/kak-zaschischatsya-ot-insaidera

8. Контроль використання USB–накопичувачів в Windows Server 2008 [Електронний ресурс]. – Режим доступу до ресурсу: https://it–

community.in.ua/2014/08/kontrol–ispolzovaniya–usb–nakopitelej–v–windows–server–2008.html/

9. Контроль використання зовнішніх пристроїв штатними засобами Windows [Електронний ресурс]. – Режим доступу до ресурсу: https://wpconfig.ru/?p=1017

10. Налаштування аудиту в Windows для повноцінного SOC-моніторингу [Електронний ресурс]. – Режим доступу до ресурсу: https://www.anti-malware.ru/practice/methods/Setting-up-auditing-in-Windows-for-full-SOC-monitoring