МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ЗАСОБИ ПОПЕРЕДЖЕННЯ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА НА ОСНОВІ ТЕХНОЛОГІЇ DLP ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Валентин ЮХИМЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. БСД-43

Валентин ЮХИМЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Сергій ЗИБІН
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри ННІЗІ
_____ Галина ГАЙДУР
“____” _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Юхименко Валентин Михайлович
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Засоби попередження витоку конфіденційної інформації підприємства на основі технології DLP ”,
Керівник кваліфікаційної роботи Сергій ЗИБІН,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *Інформаційна безпека підприємств, міжнародні стандарти (ISO/IEC 27001, GDPR тощо), наукова та технічна література з DLP-технологій, методичні матеріали щодо роботи з Digital Guardian, , управлінню політиками, моніторингу та діагностиці.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити проблематику захисту конфіденційної інформації в організаціях з обмеженими ресурсами, включаючи особливості впровадження DLP-систем.
4.2. Проаналізувати функціональні можливості, архітектуру та принципи дії сучасних DLP-систем, зокрема Digital Guardian.
4.3. Розробити практичні рекомендації щодо впровадження Digital Guardian: встановлення агента, налаштування політик, тестування системи, збір та аналіз журналів подій, з урахуванням обмежень малого та середнього бізнесу.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури з інформаційної безпеки та технологій DLP.	29.03.2025	
3.	Дослідження принципів роботи та архітектури DLP-систем.	08.04.2025	
4.	Аналіз функцій та можливостей сучасних DLP-рішень, зокрема Digital Guardian.	22.04.2025	
5.	Проєктування моделі захисту конфіденційної інформації з використанням DLP.	08.05.2025	
6.	Встановлення та налаштування агента Digital Guardian, конфігурація політик, збір діагностичних даних.	20.05.2025	
7.	Тестування DLP-системи, оцінка ефективності виявлення витоків, аналіз результатів.	22.05.2025	
8.	Оформлення тексту кваліфікаційної роботи.	03.06.2025	
9.	Підготовка презентації до захисту.	03.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Валентин ЮХИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Сергій ЗИБІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

РЕФЕРАТ

Кваліфікаційна бакалаврська робота присвячена дослідженню технологій захисту підприємств від витоку конфіденційної інформації з використанням систем запобігання витоку даних (DLP). Особливу увагу приділено аналізу функціональних можливостей та практичному застосуванню DLP-рішення Digital Guardian. Робота складається зі вступу, трьох розділів, які включають n рисунків, висновків та списку використаних джерел із n найменувань. Загальний обсяг роботи становить n аркушів, з яких n аркуші займають додатки, скріншоти та конфігураційні файли.

Метою роботи є оцінювання ефективності використання сучасних DLP-систем та впровадження практичного рішення на базі Digital Guardian для здійснення контролю витоку інформації на кінцевих точках.

Об'єктом дослідження є процеси захисту інформаційної системи від витоку конфіденційних даних.

Предмет дослідження – методи моніторингу, аудиту та блокування витоків даних, DLP-технології.

***Методи дослідження*:**

1. Аналіз технічної документації, наукових джерел та стандартів інформаційної безпеки.
2. Порівняльний аналіз DLP-рішень на ринку (Symantec, McAfee, Forcepoint, Digital Guardian).
3. Моделювання ситуацій витоку даних через кінцеві точки.
4. Практичне розгортання та тестування агента Digital Guardian на Windows-системі, управління політиками через DGMC, аналіз результатів виявлення загроз та взаємодії з DG Support.

Галузь використання – кібербезпека.

DLP, ВИТІК ДАНИХ, DIGITAL GUARDIAN, ІНФОРМАЦІЙНА БЕЗПЕКА, КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ, DGMC, АГЕНТ, ПОЛІТИКИ БЕЗПЕКИ, МОНІТОРИНГ, АУДИТ.

ABSTRACT

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному цифровому середовищі забезпечення конфіденційності даних є критично важливим аспектом інформаційної безпеки підприємств. Витоки чутливої інформації, спричинені як зовнішніми атаками, так і внутрішніми загрозами, можуть призводити до значних репутаційних та фінансових втрат. Особливо вразливими до таких ризиків є малі та середні компанії, які часто не мають достатніх ресурсів для побудови комплексних систем захисту.

Одним із дієвих рішень для контролю та попередження витоку інформації є впровадження DLP-систем (Data Loss Prevention). Вони дозволяють моніторити, блокувати або записувати передачу конфіденційних даних, як у межах локальної мережі, так і за її межами. З-поміж сучасних рішень особливу увагу привертає система Digital Guardian, яка відома своєю гнучкістю, розширеним функціоналом і можливістю точного контролю дій користувачів на кінцевих точках.

Актуальність цього дослідження зумовлена необхідністю створення ефективних, адаптивних і доступних засобів попередження витоку даних на підприємствах, що мають обмежені фінансові, кадрові й технічні ресурси. Практичне впровадження системи Digital Guardian дозволяє досягти високого рівня контролю без значного перевантаження інфраструктури, що є особливо цінним для малого й середнього бізнесу.

Таким чином, дослідження можливостей та практичного застосування DLP-технологій на прикладі Digital Guardian є науково та практично обґрунтованим завданням, спрямованим на підвищення безпеки сучасних інформаційних систем і мінімізацію ризиків витоку конфіденційної інформації.

Мета роботи є аналіз можливостей сучасних DLP-систем, оцінка ефективності їхнього використання на підприємствах та впровадження практичного рішення на базі Digital Guardian для контролю витоку інформації на кінцевих точках.

Об'єкт дослідження є інформаційно-комунікаційна система підприємства, яка потребує захисту від витоку конфіденційних даних.

Предмет дослідження – DLP-технології, їх функціональні компоненти, методи моніторингу, аудиту та блокування витоків даних.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати сучасний стан захисту конфіденційної інформації в організаціях, зокрема в малому та середньому бізнесі.
2. Дослідити вимоги міжнародних стандартів (ISO/IEC 27001, NIST, GDPR) щодо запобігання витоку даних.
3. Вивчити принципи функціонування, архітектуру та основні компоненти DLP-систем.
4. Провести практичне розгортання агента Digital Guardian, налаштування політик безпеки та моніторинг подій.

Розробити рекомендації щодо впровадження DLP-системи в умовах обмежених ресурсів підприємства.

Методи дослідження. У роботі застосовано аналіз нормативної документації та технічної літератури, методи порівняльного аналізу DLP-рішень, моделювання інфраструктури інформаційної безпеки, практичне впровадження компонента Digital Guardian, тестування виявлення витоків та оцінка ефективності системи.

Практичне значення одержаних результатів Результати дослідження можуть бути використані для впровадження на підприємствах ефективної системи захисту конфіденційної інформації на основі DLP. Використання Digital Guardian дозволяє забезпечити контроль дій користувачів, запобігати витоку даних через кінцеві точки та досягти відповідності міжнародним вимогам безпеки навіть в умовах обмежених ресурсів.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ VPN

1.1 Загрози та канали витоку конфіденційної інформації

У наш час, коли цифрові технології відіграють ключову роль у всіх сферах життя, питання збереження даних набуває особливої актуальності. Щодня створюється величезна кількість інформації, яка згодом потрапляє до інформаційно-комунікаційних систем і стає доступною широкому колу користувачів. У таких умовах захист даних від втрати повинен бути серед пріоритетів для всіх, хто працює з інформацією, особливо для бізнесу. Навіть незначний збій може призвести до порушень у роботі систем або вплинути на стабільність бізнес-процесів. Простої обходяться компаніям дорого, тож запобігання втраті даних — це критично важливе завдання.

Змішаний формат роботи, коли співробітники чергують офіс із домом, посилює ймовірність порушень у системах безпеки та появи ризиків. Великі компанії приваблюють кіберзлочинців через обсяг інформації, якою володіють, тоді як малі — через слабші системи захисту.

Сучасні технології пропонують чимало інструментів для захисту інформації, але їх ефективність напряму залежить від людського фактора — тобто від тих, хто відповідає за контроль і керування цими системами. Успішна стратегія кібербезпеки повинна враховувати як технічні рішення, так і організаційні підходи, незалежно від масштабів бізнесу чи сфери його діяльності.

На рисунку 1.1 зображено ключові чинники, що лежать в основі політики запобігання втратам даних. Ці фактори мають бути враховані у будь-якій компанії, яка прагне уникнути втрати важливої інформації [1].

Однією з основних загроз залишається зростання кількості зовнішніх атак. Попри серйозне ставлення компаній до захисту даних, зловмисники постійно

вдосконалюють свої методи й знаходять нові шляхи проникнення в системи. Це змушує організації безперервно шукати нові способи виявлення та усунення таких загроз.

Ще одна не менш небезпечна категорія — це внутрішні загрози. Найчастіше ними стають недобросовісні працівники, які свідомо намагаються зашкодити компанії зсередини, діючи самостійно або у змові з третіми особами.

Оскільки внутрішні працівники вже мають доступ до корпоративних даних і можуть володіти конфіденційною інформацією про колег або внутрішні процеси компанії, потенційна шкода від таких загроз може бути значно серйознішою, ніж від зовнішнього втручання. Особливо небезпечно, коли мова йде про високопосадовців, адже вони, як правило, мають доступ до критично важливої інформації, що охоплює стратегічні плани, фінансові дані та особисті відомості про персонал. У разі зловживання таким доступом наслідки можуть бути масштабними як для безпеки даних, так і для репутації компанії.

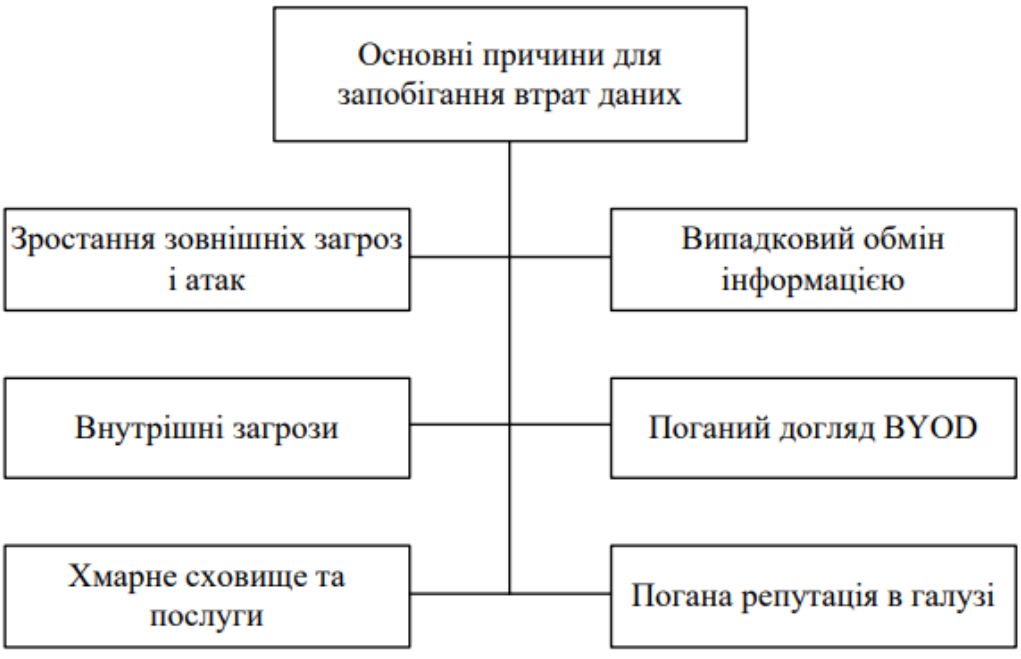

Рисунок 1.1 – Основні мотиви для впровадження політики збереження інформації

Випадкове розголошення інформації

У деяких випадках співробітники можуть ненавмисно скомпрометувати дані компанії, не маючи жодного злого умислу. Часто причиною таких інцидентів стає соціальна інженерія — одна з найпоширеніших тактик, яку використовують кіберзлочинці. Зловмисник зазвичай обирає конкретного працівника як об’єкт маніпуляцій, попередньо детально вивчивши його поведінку, звички чи слабкі місця. У ході спілкування чи взаємодії з ним жертва, нічого не підозрюючи, може надати доступ до конфіденційної інформації.

Недоліки політики BYOD

Концепція BYOD (Bring Your Own Device — «використання власних пристроїв») дозволяє працівникам користуватись особистими телефонами, ноутбуками або планшетами для роботи з корпоративними ресурсами. Попри зручність і підвищення продуктивності, така практика несе серйозні ризики для інформаційної безпеки. Особливо вразливими є компанії, які не мають чітко налагоджених механізмів контролю або взагалі не впровадили політики BYOD. Якщо не передбачено відповідних протоколів безпеки, співробітники можуть ненавмисне передавати або зберігати важливі дані на ненадійних пристроях, не усвідомлюючи можливих наслідків [1-2].

Ризики використання хмарних сервісів

Ще однією поширеною практикою є використання особистих облікових записів у хмарних сховищах, таких як Google Drive або Dropbox, для збереження чи обміну службовою інформацією. Такий підхід особливо небезпечний у компаніях, де працівники не проходять навчання щодо безпечної роботи з даними або не мають чітких інструкцій. Відповідальність за запровадження надійної системи безпеки лежить на організації — саме вона має забезпечити обмежений доступ до корпоративних даних лише через внутрішню інфраструктуру, з належними правами доступу та авторизацією.

Репутаційні втрати

Недостатній рівень кіберзахисту та повторювані інциденти з компрометацією даних можуть швидко зруйнувати репутацію компанії на ринку. У таких випадках клієнти часто переходять до конкурентів, навіть якщо раніше

були відданими бренду. Для бізнесу це означає не лише втрату довіри, а й реальні фінансові збитки.

Існує багато технологій, що допомагають протидіяти загрозам і забезпечують зовнішній захист інформації (рис. 1.2). Особливу роль у внутрішній безпеці відіграють DLP-системи (Data Loss Prevention), які спрямовані на виявлення і запобігання витокам даних саме всередині організації.

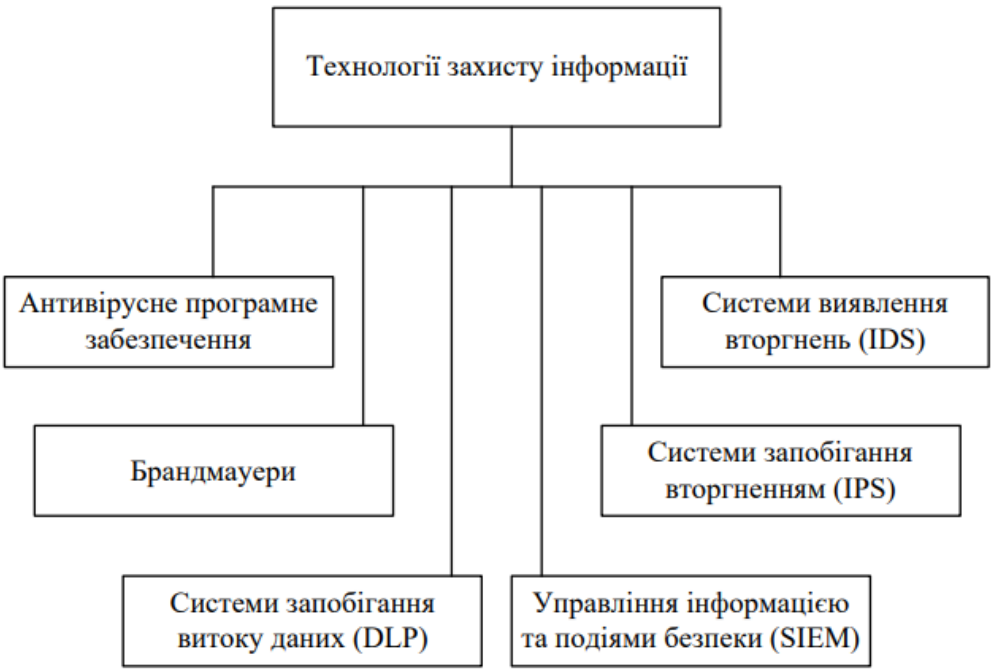

Рисунок 1.2 – Комплекс технологій для забезпечення інформаційної безпеки

Джерела загроз в інформаційній безпеці

Під джерелами загроз у сфері інформаційної безпеки розуміють чинники, які можуть спричинити негативний вплив на критично важливі інтереси особи, суспільства та держави у цифровому просторі.

Загроза — це будь-яка подія або сукупність обставин, здатна призвести до порушення політики захисту інформації або завдати шкоди інформаційній системі.

Загрози, їх джерела (включно зі зловмисниками), методи протидії та підходи до оцінки ефективності заходів безпеки суттєво відрізняються залежно від рівня, на якому функціонує інформаційно-телекомунікаційна система. Саме

тому для належного захисту даних та стабільного функціонування систем важливо класифікувати елементи інформаційної інфраструктури за рівнями.

Ключові рівні інформаційної інфраструктури [3]:

- Операційні системи – програмне середовище, що забезпечує базове управління апаратним забезпеченням.
- Мережеві сервіси та прикладні програми – програмне забезпечення, що підтримує взаємодію між користувачами та мережами.
- Системи управління базами даних (СУБД) – інструменти для зберігання, обробки та організації даних.
- Фізичний рівень – канали зв’язку, апаратне забезпечення, технічна інфраструктура.
- Мережеве обладнання – пристрої, що забезпечують передачу та маршрутизацію даних (комутатори, маршрутизатори, концентратори тощо).
- Бізнес-процеси організації – операційна діяльність компанії, яка тісно пов’язана з використанням та обробкою інформації.

1. Фізичний рівень, мережевий рівень та рівень мережевих сервісів

- Зовнішні загрози: до цієї категорії належать сторонні особи, що поширюють віруси, шкідливе програмне забезпечення, а також хакери та інші порушники, які намагаються отримати несанкціонований доступ до систем.
- Внутрішні загрози: працівники, які діють у межах своїх посадових обов’язків або виходять за їх межі, зокрема ті, хто має доступ до мережевого обладнання чи адмініструє відповідні сервіси.
- Комбіновані загрози: випадки, коли внутрішні та зовнішні суб’єкти діють узгоджено або в змові, посилюючи ефект атаки.

2. Рівень операційних систем, СУБД та технологічних процесів

- Внутрішні загрози: адміністратори операційних систем, баз даних або фахівці з інформаційної безпеки, які можуть зловживати своїми правами доступу або порушувати встановлені політики безпеки.

- Комбіновані загрози: зловмисна взаємодія між внутрішніми працівниками та зовнішніми особами з метою спільної атаки чи витоку даних.

3. Рівень бізнес-процесів

- Внутрішні загрози: авторизовані користувачі, оператори автоматизованих банківських систем (АБС), менеджери або інші працівники, які можуть свідомо чи несвідомо порушити правила безпеки.
- Комбіновані загрози: співпраця внутрішніх працівників з зовнішніми сторонами, наприклад, конкурентами, з метою отримання переваги або компрометації компанії [3].

1.2 Роль DLP-технологій у забезпеченні інформаційної безпеки підприємства

Актуальні зовнішні загрози інформаційної безпеки

Хакерські атаки дедалі частіше розглядаються на міжнародному рівні як складова глобальної загрози, що супроводжує перехід суспільства до «цифрової епохи». Сьогодні від кіберзлочинності не застраховані навіть малі підприємства — особливо ті, що працюють як підрядники або постачальники для великих компаній і мають доступ до цінних даних. Також уразливими залишаються інтернет-магазини та невеликі провайдери, які все частіше стають жертвами DDoS-атак, що блокують їхню онлайн-діяльність.

Серед найбільш поширених зовнішніх загроз:

- Викрадення конфіденційних даних шляхом злому інформаційної системи або використання ненадійних каналів передачі. Найефективнішим засобом протидії витокам даних є DLP-системи, однак не всі компанії малого і середнього бізнесу мають ресурси для їх впровадження.
- Викрадення персональних даних через компрометацію систем ідентифікації та подальший продаж інформації на тіньовому ринку. Такий ризик особливо актуальний для банків та сервісних організацій, які працюють із великими обсягами даних клієнтів [4].

- Інсайдерське викрадення комерційної інформації з ініціативи конкурентів — зазвичай це стосується баз даних клієнтів або інших бізнес-критичних матеріалів.
- DDoS-атаки, що паралізують комунікаційні канали та роботу онлайн-сервісів. Для компаній, які працюють через інтернет, такі атаки можуть мати критичні наслідки.
- Вірусне зараження, зокрема віруси-шифрувальники, які блокують доступ до даних і вимагають викуп — найчастіше у криптовалюті, щоб ускладнити відстеження транзакцій.
- Дефейс сайтів — заміна головної сторінки веб-ресурсу іншим, часто образливим або політично вмотивованим контентом.
- Фішинг — обман користувачів через підроблені листи або вебсторінки, з метою викрадення паролів чи фінансової інформації.
- Спам-атаки, які перевантажують поштові скриньки, ускладнюючи отримання важливої кореспонденції [5].
- Соціальна інженерія — маніпулятивні дії зловмисників, які змушують співробітників компанії добровільно надати доступ або ресурси.
- Втрати даних через апаратні збої, технічні несправності, стихійні лиха або інші аварійні ситуації, що можуть призвести до незворотної втрати інформації.

Сучасний ландшафт кіберзагроз: тенденції та виклики

Попри зміну технічних умов, загальний перелік загроз інформаційній безпеці залишається стабільним, натомість постійно вдосконалюються способи їх реалізації. Вразливості в стандартних компонентах інформаційних систем — таких як операційні системи чи мережеві протоколи — не завжди усуваються оперативно. Наприклад, уразливості в Windows XP залишались відкритими близько двох років, перш ніж Microsoft випустила відповідні оновлення. За цей час хакери вже активно використовували їх у своїх атаках.

Зловмисники уважно відстежують нові оновлення і миттєво перевіряють, як зміни впливають на захищеність систем. Окрім того, зростає доступність

інструментів для атак — сучасні машинні технології настільки спростились, що їх можуть використовувати навіть недосвідчені користувачі. Наприклад, сьогодні можна за $10 придбати підписку на онлайн-сервіс для перевірки вразливостей і за лічені хвилини ініціювати DDoS-атаку на малозахищений сервер. Це може повністю паралізувати роботу сайту і зробити його недоступним для клієнтів.

Унікальною рисою сьогодення є активне залучення до атак пристроїв Інтернету речей — побутових приладів, відеокамер, навіть холодильників або кавоварок. Через економію коштів на захисті ПЗ, виробники часто не впроваджують належні механізми безпеки в ці пристрої, що робить їх легкою мішенню для атак типу botnet.

Не менш серйозну загрозу становлять і внутрішні порушення, особливо з боку співробітників, які не крадуть інформацію, а навмисно змінюють її для досягнення особистих або фінансових цілей. Одним із прикладів є маніпуляція даними в базах для полегшення крадіжки ресурсів. Зокрема, підвищення температури зберігання пального може призвести до штучного збільшення його об’єму в резервуарах, що дозволяє відкачати частину продукту без спрацювання датчиків. Таке втручання можливе лише при отриманні несанкціонованого доступу до систем, які керують температурним режимом на складах.

Ключові загрози інформаційній безпеці підприємства

У сучасних умовах навіть успішне та добре організоване підприємство може стати об’єктом цілеспрямованих атак, спрямованих на компрометацію або викрадення важливої інформації. До основних загроз, які можуть поставити під загрозу стабільну роботу компанії, належать:

- Несанкціонований доступ та витік даних. Крадіжка інформації — одна з найпоширеніших загроз. Наприклад, дані, що зберігаються у програмі 1С або іншому програмному забезпеченні, можуть бути скопійовані таємно, без явних ознак втручання [5-7].
- Хакерські атаки. Це комплекс дій, спрямованих на виявлення вразливостей у цифрових системах — від комп’ютерів і смартфонів до цілих

мереж підприємства. Часто хакери користуються недоліками у програмному забезпеченні, тому важливо застосовувати тільки ліцензовані та регулярно оновлювані продукти. Хоча не всі хакери діють зловмисно, у сучасному дискурсі цей термін асоціюється саме з кіберзлочинністю.

- Людський фактор і халатність. Недбалість співробітників, нехтування правилами безпеки або ненавмисні помилки можуть стати причиною серйозних проблем у системі безпеки.
- Шкідливе програмне забезпечення (ПЗ). Віруси, трояни, шпигунські програми, програми-вимагачі здатні завдати значної шкоди: викрадати, шифрувати або знищувати дані, блокувати системи, чи навіть повністю паралізувати роботу компанії. Особливо небезпечні програми-вимагачі, які вимагають викуп за відновлення доступу до інформації, часто — у криптовалюті.
- Спам-розсилки. Масова розсилка небажаної або фальшивої інформації, що може містити фішингові посилання або віруси. Навіть один необережний клік співробітника може призвести до зараження всієї мережі.
- Технічні збої. Відмова в роботі апаратного або програмного забезпечення, яку можуть усунути лише фахівці з інформаційної безпеки, — ще один серйозний ризик.
- Фінансові шахрайства. Кіберзлочинці можуть здійснювати атаки з метою заволодіння грошима компанії або зірвати важливі фінансові операції.
- Крадіжка обладнання. Фізичне викрадення комп’ютерів чи серверів не лише впливає на продуктивність, але й часто супроводжується втратою критично важливої інформації.

Найнебезпечнішими загрозами для підприємств вважаються саме шкідливе програмне забезпечення та витоки конфіденційної інформації.

Щоб мінімізувати ці ризики, компанії мають системно підходити до питань кібербезпеки. До пріоритетних заходів належать:

- регулярне навчання персоналу з основ інформаційної безпеки;
- встановлення антивірусного захисту та фільтрації небажаного контенту;
- проведення ІТ-аудиту;

- постійний моніторинг IT-середовища підприємства та його вразливостей.

1.3 Огляд сучасних DLP-рішень та класифікація систем запобігання витоку даних

Класифікація DLP-систем та особливості їх використання

1. За характером контролю: активний і пасивний

– Системи з активним контролем здатні блокувати передачу інформації, яка ідентифікована як конфіденційна. Вони ефективні при захисті від випадкових витоків даних, але можуть призвести до призупинення окремих бізнес-процесів через хибні спрацювання.

– Системи з пасивним контролем не блокують передачу даних, а лише фіксують порушення. Вони не впливають на бізнес-процеси, але підходять переважно для виявлення систематичних порушень політики безпеки.

2. За архітектурною побудовою: шлюзові та хостові

– Шлюзові DLP-системи встановлюються на проміжних серверах і аналізують трафік, що проходить через мережу [7].

– Хостові DLP-системи базуються на спеціальних агентах, які інсталюються безпосередньо на робочі комп’ютери користувачів і контролюють дії в межах локального середовища.

На практиці найбільш ефективною є гібридна модель, яка поєднує шлюзові та хостові компоненти, забезпечуючи всебічний моніторинг і контроль.

3. Гравці ринку DLP-рішень

Серед провідних постачальників DLP-систем варто відзначити компанії, що вже мають визнання у сфері кібербезпеки:

- Endpoint Protector by CoSoSys
- Symantec DLP
- McAfee DLP
- Forcepoint DLP
- SecureTrust DLP

Обсяг світового ринку DLP-рішень наразі оцінюється приблизно в 400 мільйонів доларів, що значно менше порівняно з ринком антивірусного ПЗ. Водночас галузь демонструє динамічне зростання — ще у 2009 році цей показник становив лише трохи більше 200 мільйонів.

Endpoint Protector by CoSoSys: сучасне рішення для захисту кінцевих точок

Компанія CoSoSys пропонує своє DLP-рішення Endpoint Protector у кількох форматах — як локальне програмне забезпечення, як хмарну послугу або як окремий інсталяційний пакет.

У локальній версії система забезпечує захист пристроїв на базі Windows, macOS та Linux. Центральний елемент рішення — Endpoint Protector Server — здійснює мережеву взаємодію з клієнтськими агентами, встановленими на кожній кінцевій точці.

Окрім захисту комп’ютерів, система контролює зовнішні носії та пристрої, зокрема USB-накопичувачі, цифрові камери та інші периферійні пристрої. Крім того, існує можливість розгортання рішення у вигляді віртуального апарата на приватному сервері організації, що дозволяє більш гнучко налаштовувати інфраструктуру безпеки.

Інтерфейс Endpoint Protector by CoSoSys продемонстровано на рис. 1.3.

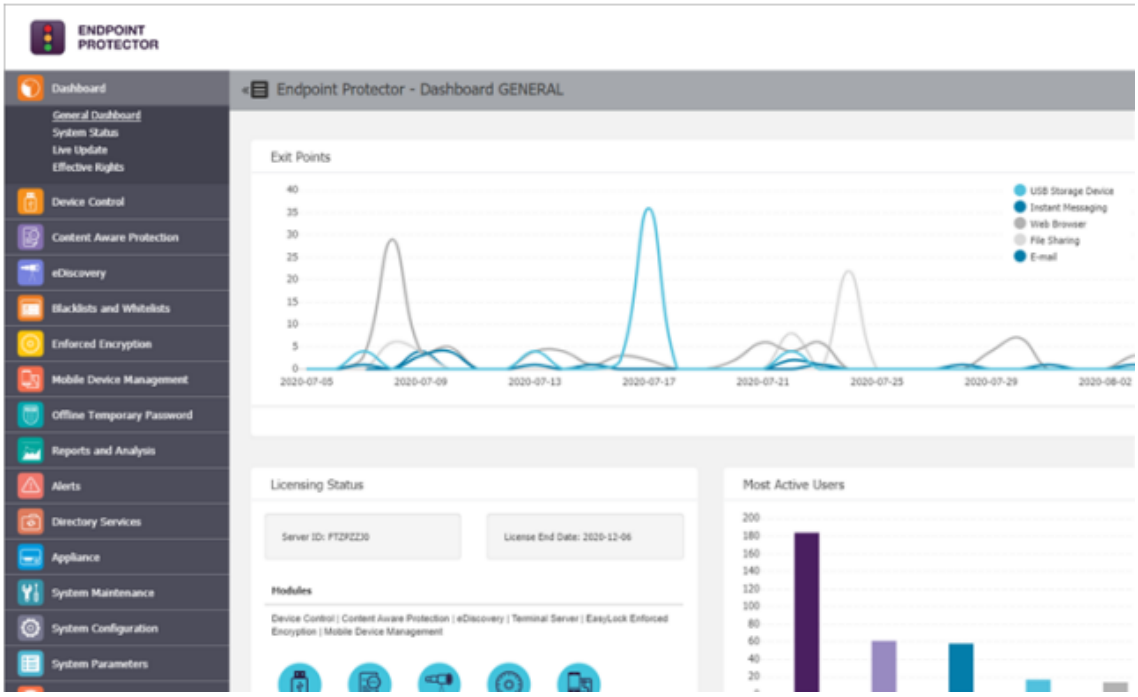

Рисунок 1.3 – Головна панель управління в Endpoint Protector

Основні особливості:

- Платформа захисту Endpoint Protection.
- Реалізація у вигляді пристрою, локального програмного забезпечення або SaaS-рішення (програмне забезпечення як послуга).
- Відповідність ключовим міжнародним стандартам: HIPAA, PCI DSS, GDPR.
- Підтримка захисту підключених пристроїв (USB, цифрові носії тощо).
- Можливість примусового шифрування даних.

Повна версія Endpoint Protector забезпечує:

- контроль та захист вмісту;
- управління доступом до пристроїв;
- примусове шифрування переданих даних;
- мережеве виявлення пристроїв;
- керування мобільними пристроями [8].

Для невеликих інфраструктур доступна автономна версія, яка дозволяє захищати одну кінцеву точку на інсталяцію. Базова конфігурація — Endpoint Protector Basic — включає модулі контролю пристроїв та контенту.

Крім того, користувачам доступний My Endpoint Protector — хмарний пакет, який дозволяє уникнути власної інфраструктури і включає:

- захист вмісту,
- контроль пристроїв,
- управління мобільними пристроями.

Усі версії рішення забезпечують відповідність міжнародним вимогам з інформаційної безпеки (HIPAA, PCI DSS, GDPR).

Контроль вмісту та пристроїв

Функціонал захисту вмісту дозволяє керувати передачею файлів відповідно до політик безпеки, встановлених адміністратором. Залежно від заданих правил:

- можна повністю блокувати передачу файлів для окремих груп користувачів;
- або дозволяти пересилання лише тих файлів, які відповідають визначеним критеріям.

Аналогічно працює система контролю пристроїв: вона може повністю заборонити підключення зовнішніх носіїв, або ж дозволити їх використання у контрольованих умовах.

Symantec DLP: комплексне рішення для контролю даних і дій користувачів

Система Symantec DLP поєднує функціональність моніторингу користувацької активності з інструментами управління ризиками, пов’язаними з обробкою даних. Рішення дозволяє здійснювати повноцінне відстеження розташування та руху конфіденційної інформації незалежно від того, де вона зберігається: на локальних серверах, настільних комп’ютерах, мобільних пристроях або у хмарному середовищі [9].

Однією з ключових функцій системи є автоматичне виявлення чутливих даних при першому налаштуванні. Після цього адміністратор отримує можливість:

- централізовано перемістити ці дані на захищений сервер;
- зберегти їх у безпечному сховищі;

– або застосувати політики захисту безпосередньо на місці їхнього зберігання.

У результаті формуються індивідуальні шаблони політик та робочі процеси, які допомагають підприємству відповідати таким вимогам міжнародної інформаційної безпеки, як HIPAA, GDPR та PCI DSS.

Інтерфейс системи Symantec DLP представлено на рис. 1.4.

Рисунок 1.4 – Панель адміністрування Symantec DLP

Основні характеристики Symantec DLP

Рішення Symantec Data Loss Prevention (DLP) — це потужний інструмент для захисту конфіденційної інформації на всіх рівнях корпоративної IT-інфраструктури. Система забезпечує:

– Відстеження користувацької активності: фіксується кожен випадок доступу до чутливої інформації, включно з обліковими записами, які стали причиною спрацювання політик безпеки.

– Інтегроване шифрування: усі конфіденційні документи шифруються, доступ до них надається виключно авторизованим користувачам.

– Відповідність міжнародним стандартам: система підтримує вимоги HIPAA, GDPR та PCI DSS.

Symantec DLP забезпечує повне знищення видалених або відкинутих копій документів — без можливості їхнього відновлення з тимчасових файлів або кешу. Навіть у разі передавання даних на мобільні або віддалені пристрої, вони залишаються захищеними [9].

Ключові функції:

– Цифрове маркування копій: кожен екземпляр документа позначається цифровим "відбитком", що дозволяє відстежувати його рух.

– Обмеження на переміщення та копіювання: за допомогою політик безпеки забороняється надсилання файлів електронною поштою, їх завантаження в інтернет або переміщення через мережу без дозволу.

– Захист кінцевих точок: система є складовою частиною комплексної безпеки робочих станцій, здатна виявляти зловмисні програми або вторгнення, які можуть загрожувати даним.

– Моніторинг несанкціонованого ПЗ: фіксується встановлення сторонніх програм, особливо якщо вони працюють на пристроях, які використовуються для доступу до корпоративних даних — зокрема у випадках використання BYOD (Bring Your Own Device).

McAfee DLP: універсальне рішення для захисту даних у всіх середовищах

Компанія McAfee розробила інтегровану DLP-платформу, що забезпечує захист даних у локальній мережі, хмарних сервісах і на кінцевих пристроях. Рішення пропонує централізоване управління політиками безпеки та надає зручні інструменти для реагування на інциденти — з можливістю налаштування робочих процесів відповідно до потреб організації.

Гнучкі варіанти розгортання дозволяють адаптувати систему під специфіку як малих, так і великих IT-інфраструктур, зберігаючи ефективність і масштабованість.

Інтерфейс системи McAfee DLP представлено на рис. 1.5.

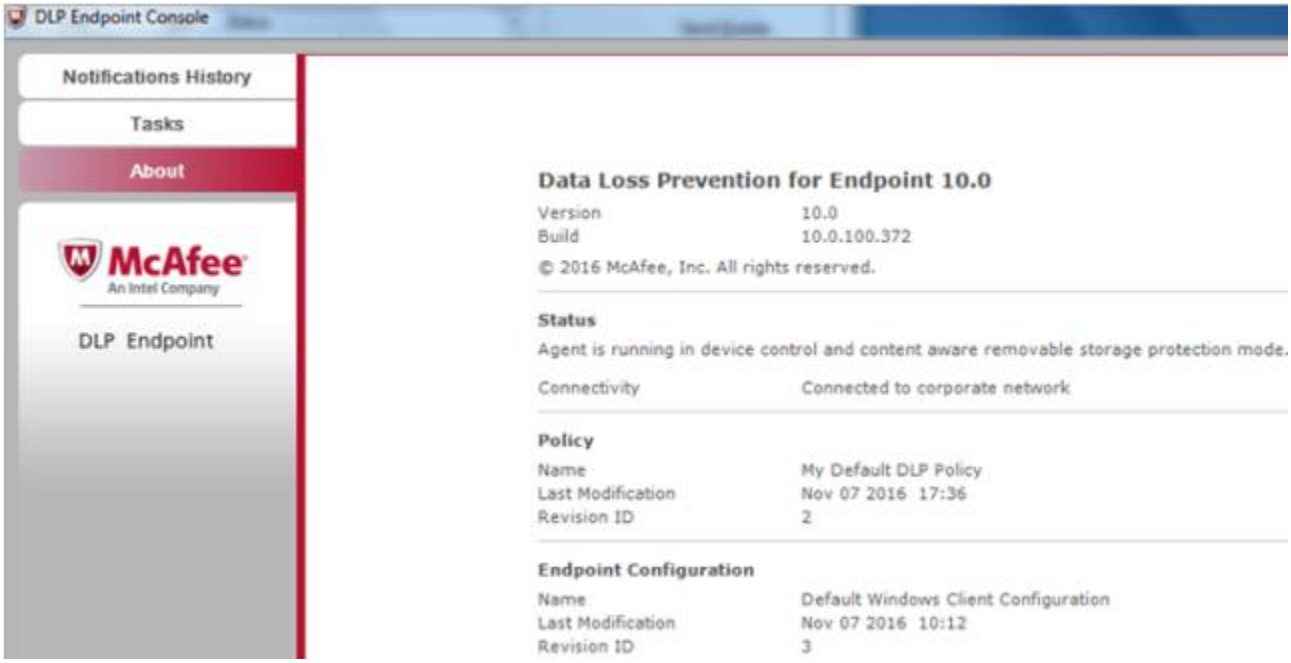

Рисунок 1.5 – Робоче середовище рішення McAfee Data Loss Prevention

Рішення McAfee Data Loss Prevention вирізняється широкими можливостями моніторингу, класифікації та захисту інформації в усіх середовищах — як локальних, так і хмарних. Його функціональність дозволяє не лише виявляти потенційні загрози, а й оперативно реагувати на них у режимі реального часу.

Ключові можливості [10]:

- Розширене виявлення активності: завдяки технології глибокого захоплення, система забезпечує повну видимість дій користувачів і даних, дозволяючи зрозуміти, як саме інформація використовується, куди передається і як може витікати.
- Потужна класифікація даних: McAfee DLP має вдосконалений механізм виявлення та категоризації чутливої інформації, що дозволяє точніше формувати політики безпеки.
- Гнучка реакція на порушення політик: система може автоматично застосовувати захисні заходи до даних, що порушують правила — шифрувати, перенаправляти, блокувати або поміщати у карантин.

Централізоване керування та звітність

McAfee DLP пропонує єдину панель управління для моніторингу інцидентів і формування аналітики. Політики безпеки, що застосовуються у локальних середовищах і в хмарі, синхронізуються через централізовану консоль McAfee, що забезпечує цілісне управління інформаційною безпекою.

Forcepoint DLP: адаптивна система захисту даних з поведінковим аналізом

Forcepoint Data Loss Prevention — це інтелектуальне рішення, орієнтоване на гнучкий, персоналізований захист даних. Система адаптується до контексту дій користувача, блокуючи лише ті операції, які становлять реальну загрозу, що дозволяє зберігати продуктивність працівників без шкоди для безпеки.

Рішення відповідає міжнародним нормам і стандартам, включно з GDPR, CCPA та іншими вимогами у понад 80 країнах світу, що робить його універсальним для компаній з глобальною присутністю.

Інтерфейс системи Forcepoint DLP представлено на рис. 1.6.

Основні функціональні можливості:

- Підтримка технологій Drip DLP, Native Remediation та OCR (оптичне розпізнавання символів) — що дозволяє захищати дані навіть у вигляді зображень або повільно "витікаючих" потоків.
- Захист структурованих і неструктурованих даних — зокрема PII (персональна інформація), PHI (медичні дані), фінансові записи, інтелектуальна власність, дані кредитних карток тощо.
- Попередньо налаштовані політики безпеки — широка бібліотека шаблонів дозволяє швидко реалізувати захист даних відповідно до типових потреб компаній.
- Поведінкова аналітика та адаптація до ризику — система вивчає поведінку користувачів і застосовує політики на основі рівня ризику конкретних дій.
- Захист поза мережею — навіть якщо пристрої користувача не підключені до корпоративної мережі, система продовжує контролювати безпеку даних.

– Зниження навантаження на адміністратора — Forcepoint оптимізовано для мінімізації хибних спрацювань, скорочення кількості сповіщень і тривог, дозволяючи фокусуватись на дійсно критичних інцидентах.

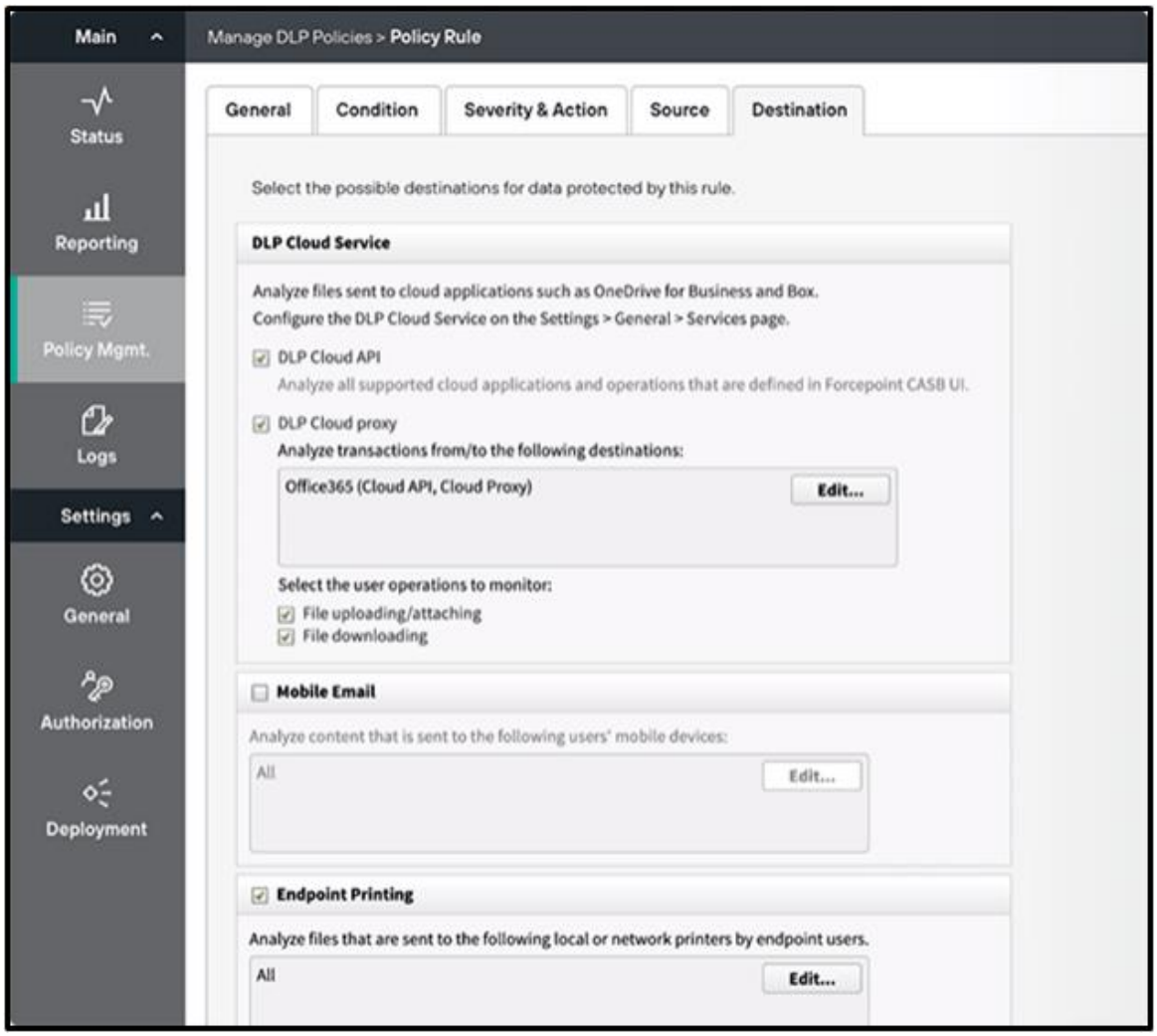

Рисунок 1.6 – Панель керування системою Forcepoint DLP

SecureTrust DLP: повний контроль над даними у будь-якому стані

Рішення SecureTrust Data Loss Prevention забезпечує виявлення, моніторинг і захист даних, незалежно від того, знаходяться вони в стані спокою (збережені), у русі (передаються) або активно використовуються. Його головна мета — запобігати ексфільтрації інформації та гарантувати відповідність вимогам нормативних актів і внутрішніх політик організації.

Інтерфейс системи SecureTrust DLP представлено на рис. 1.7.

Основні характеристики [11]:

- Захист на всіх етапах життєвого циклу даних — з моменту збереження до обробки або передавання.
- Попередньо налаштовані політики — понад 70 шаблонів політик та категорій ризику, які можна швидко активувати або деактивувати відповідно до потреб організації.
- Аналіз веб-комунікацій і вкладень — система перевіряє весь інтернет-трафік і вміст файлів на предмет порушень корпоративних стандартів, нормативів безпеки та політик допустимого використання.

SecureTrust DLP дозволяє створити надійну й масштабовану архітектуру інформаційної безпеки з акцентом на гнучкість управління, відповідність вимогам та запобігання витокам даних у реальному часі.

Рисунок 1.7 – Робочий екран системи SecureTrust DLP

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА АНАЛІЗ ЗАСОБІВ ЗАХИСТУ З ВИКОРИСТАННЯМ OPENVPN

2.1 Архітектура та принципи роботи DLP-систем

Digital Guardian DLP — це універсальне рішення для запобігання витокам даних, захисту від несанкціонованого доступу та інсайдерських загроз, яке допомагає виявляти потенційні ризики безпеки, контролювати потік інформації та забезпечувати захист конфіденційних даних. Система підтримує відповідність чинним нормативним вимогам у сфері захисту інформації, включаючи GDPR, HIPAA та інші стандарти. Digital Guardian також надає можливість отримувати миттєві сповіщення про інциденти безпеки та формувати детальні звіти, що спрощує реагування на загрози. Рішення є простим у розгортанні, масштабованим і підходить для організацій будь-якого розміру [12].

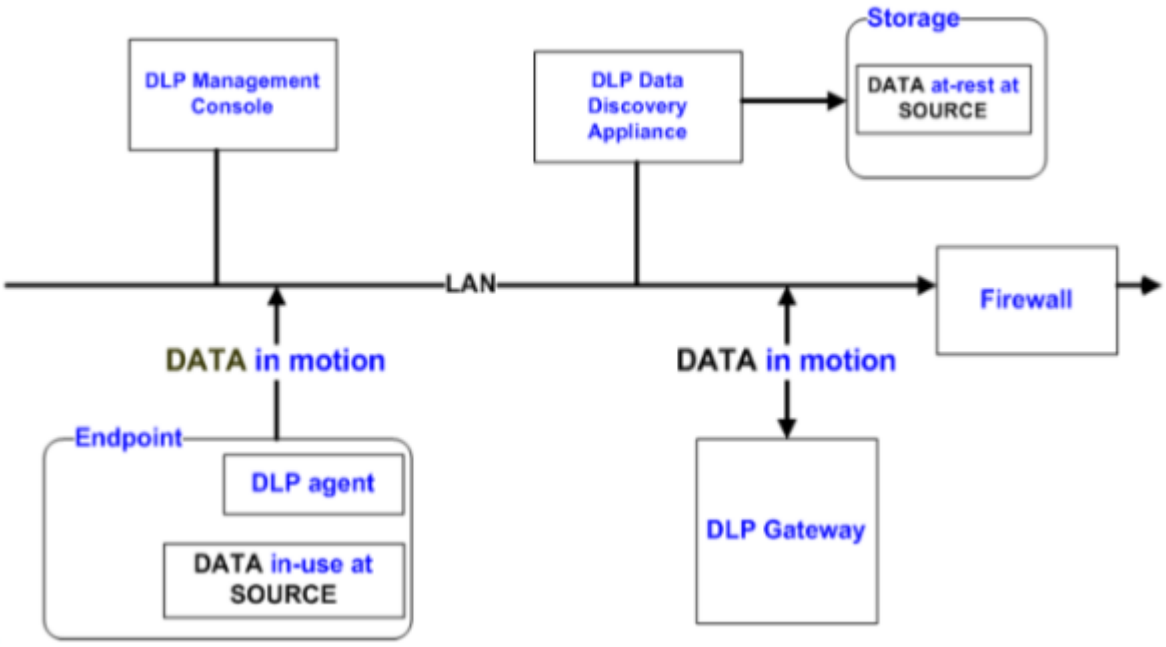

Рисунок 2.1 – Загальна схема побудови DLP-інфраструктури

Усі виявлені інциденти безпеки та журнали подій можуть автоматично передаватися до систем управління інформацією та подіями безпеки (SIEM),

таких як Splunk, IBM QRadar, LogRhythm або ArcSight, для поглибленого аналізу та розслідування. Крім того, за допомогою REST API зібрані дані можуть бути інтегровані з аналітичними платформами, такими як Power BI або Tableau, що дає змогу здійснювати розширену візуалізацію та аналіз інцидентів (рис. 2.2).

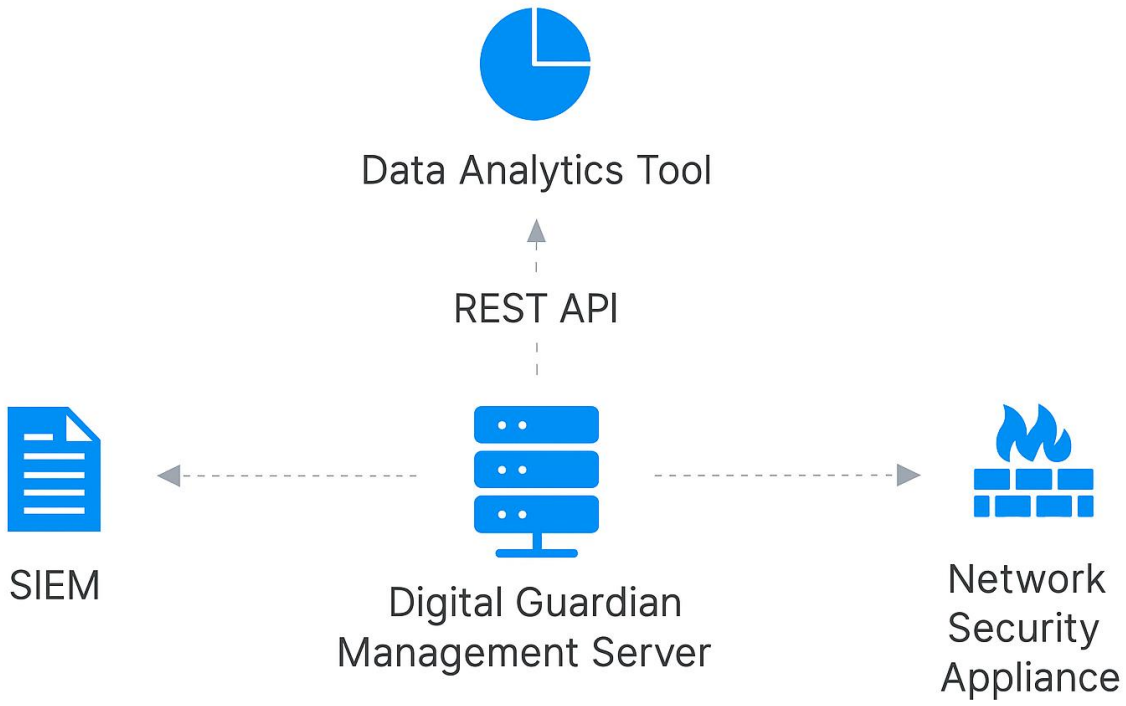

Рисунок 2.2 – Інтеграція Digital Guardian DLP з SIEM та аналітичними платформами

Digital Guardian DLP забезпечує всебічний захист конфіденційної інформації незалежно від місця її зберігання чи використання. Система здатна виявляти та контролювати широкий спектр чутливих даних, зокрема:

- персональні дані користувачів;
- стратегічні документи та бізнес-аналітику;
- бази даних клієнтів;
- платіжну інформацію (наприклад, номери кредитних карток);
- інтелектуальну власність;

- комерційні таємниці, промислові зразки, технологічні розробки;
- контракти та інші юридично значущі документи.

Рішення повністю відповідає вимогам найвідоміших стандартів і нормативних актів у сфері захисту даних, таких як ***GDPR, HIPAA, SOX, PCI DSS, GLBA, ISO/IEC 27001, CCPA***. Завдяки Digital Guardian організації можуть навчати персонал правильній роботі з конфіденційною інформацією без впливу на звичні бізнес-процеси.

Система спроектована з акцентом на простоту розгортання та оперативність налаштування — не потребує високоспеціалізованого персоналу чи додаткового обладнання. Захист критичних даних може бути активований уже впродовж кількох годин після впровадження, достатньо лише обрати безпечні канали передачі та базові політики.

Окрім цього, ***Digital Guardian DLP*** надає інструменти контролю за корпоративними мобільними пристроями, а також відстежує переміщення даних із хмарних сервісів, зокрема Microsoft Office 365 (рис. 2.3).

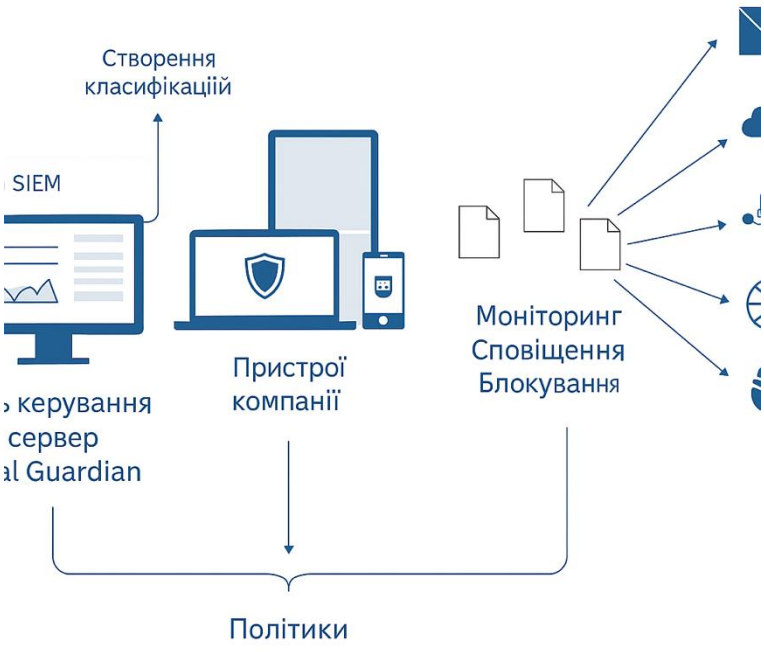

Рисунок 2.3 – Взаємодія компонентів Digital Guardian DLP з корпоративною інфраструктурою

Сервер Digital Guardian управляє базою даних, що містить інформацію про робочі станції та журнали безпеки. Консоль адміністратора надає централізований доступ для керування політиками безпеки та перегляду всієї зібраної інформації про інциденти. Усі дії користувачів реєструються, а задані політики автоматично застосовуються на всіх пристроях з встановленим агентом Digital Guardian — ПК, ноутбуках, планшетах і смартфонах [12-14].

Система захищає конфіденційні дані ще до того, як вони можуть покинути межі компанії, незалежно від способу зберігання або переміщення (рис. 2.4). Digital Guardian забезпечує зручний і зрозумілий огляд усіх потенційних загроз через єдину інтегровану консоль управління. При належному впровадженні ця система дозволяє досягти високого рівня захисту від витоків інформації та несанкціонованого доступу, а також ефективно використовується під час аудиту для виявлення конфіденційних даних в організаційних системах.

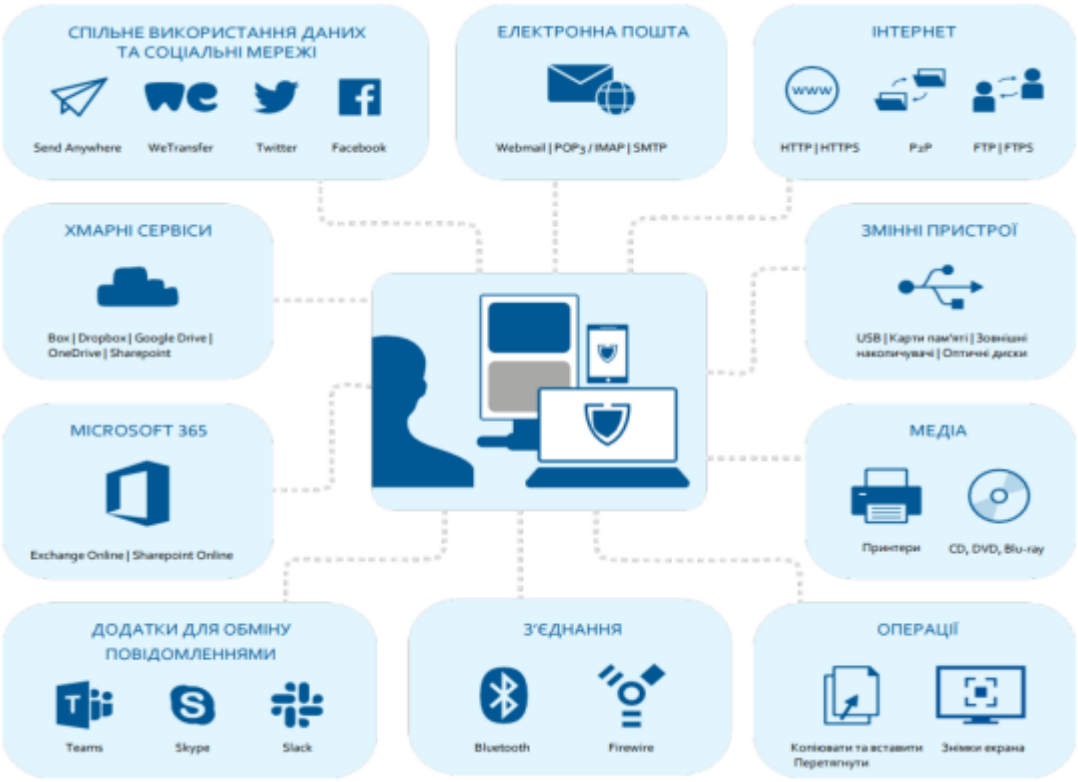

Рисунок 2.4 – Засоби виявлення і блокування витоку інформації в Digital Guardian

На рис. 2.5 представлено архітектуру DLP-системи Digital Guardian, яка демонструє взаємодію основних компонентів у процесі забезпечення захисту конфіденційної інформації в організації:

1. Кінцеві пристрої з агентом Digital Guardian (ПК і ноутбуки) — на цих пристроях встановлюється спеціальний клієнт, що реєструє дії користувачів і застосовує політики безпеки відповідно до централізованих налаштувань.

2. Центральний сервер керування та база даних (Digital Guardian Management Server + SQL) — усі дані про активність на пристроях автоматично передаються до серверної частини системи. Після підключення до мережі, клієнти синхронізуються із сервером, отримуючи актуальні політики й конфігурації.

3. Консоль адміністрування Digital Guardian — надає централізований доступ до всієї зібраної інформації, дозволяє змінювати налаштування політик, аналізувати інциденти та формувати звіти.

4. Сервери в регіональних підрозділах — Digital Guardian підтримує розподілену інфраструктуру, що дозволяє централізовано керувати політиками й моніторингом в кількох філіях компанії через одну консоль [13].

Рисунок 2.5 – Побудова інфраструктури захисту даних з Digital Guardian

Усі функції та компоненти Digital Guardian DLP — зокрема клієнтські агенти, сервери та бази даних — централізовано управляються через веб-інтерфейс або настільну консоль адміністратора. У цій консолі відображається поточний стан системи, аналітичні звіти, результати моніторингу, статистичні

дані та графіки, що дозволяє IT-фахівцям оперативно реагувати на інциденти безпеки та коригувати політики доступу й захисту в реальному часі.

Консоль управління Digital Guardian DLP має зручну та функціонально насичену структуру, що дозволяє керувати всіма компонентами системи — від клієнтських агентів до серверів і політик безпеки. У головному меню користувачі можуть перемикатися між основними модулями (наприклад, Discovery, Protection), використовуючи відповідні іконки в центральній частині інтерфейсу. У верхній частині екрана розташований перемикач між режимами Налаштувань (Settings) і Записів (Records), що використовується в модулях захисту й обслуговування: у першому режимі адміністратор може вносити зміни до політик безпеки для окремих користувачів, груп або пристроїв, а в другому — переглядати звіти, події та статистику.

Зліва розміщене дерево користувачів, у якому відображаються всі підключені до серверів об’єкти: комп’ютери, користувачі та групи. Обране підключення можна змінити у профілі адміністратора. Справа — панель доступу до компонентів системи: модулів обслуговування, профілю користувача та довідкової інформації [14].

Центральна область перегляду служить для відображення інформації та взаємодії з функціоналом системи. Вміст цієї області динамічно змінюється залежно від обраного модуля та активного режиму (налаштування або перегляду записів). Через консоль також можна отримати доступ до панелі інструментів, сповіщень, налаштування звітів, а також переглядати детальні діаграми та події безпеки. Такий підхід забезпечує повний контроль над системою безпеки в єдиному інтерфейсі, зберігаючи простоту у використанні.

2.2 Порівняння основних функціональних модулів популярних DLP-систем

Data Loss Prevention (DLP) — це комплекс технологій, процесів і інструментів, спрямованих на запобігання витоку конфіденційної інформації за межі організації. Системи DLP дозволяють виявляти, класифікувати, моніторити

й захищати чутливі дані незалежно від того, де вони зберігаються або переміщуються — на робочих станціях, у корпоративних мережах чи хмарних середовищах. Основною метою впровадження Digital Guardian DLP є встановлення повного контролю над даними, зведення до мінімуму ризику їхнього витоку або несанкціонованого доступу [15].

Основні принципи роботи DLP-систем:

1. Ідентифікація та класифікація даних.

Digital Guardian застосовує різноманітні методи виявлення конфіденційної інформації — включаючи аналіз вмісту файлів, метаданих, шаблонів даних і регулярних виразів. Це дозволяє точно визначити, які дані потребують особливого захисту, і застосувати відповідні правила до їх обробки.

2. Моніторинг і контроль дій з даними.

Система в реальному часі відстежує всі операції з даними — передачу в мережі, копіювання на зовнішні пристрої, завантаження у хмарні сервіси, друк, тощо. У випадку виявлення підозрілої активності, Digital Guardian може заблокувати дію або надіслати сповіщення адміністраторам.

3. Впровадження політик безпеки.

На основі потреб конкретної організації встановлюються політики щодо обробки конфіденційної інформації. Digital Guardian забезпечує автоматичне застосування цих політик — від обмеження доступу до даних до запобігання їх передачі за межі організації — з повною реєстрацією кожної дії.

4. Звітування та аналітика.

Системи DLP, зокрема Digital Guardian, формують детальні звіти про інциденти безпеки та надають аналітичні інструменти для оцінки ефективності політик. Це дозволяє IT-відділу не лише проводити ретельне розслідування подій, але й своєчасно оновлювати налаштування безпеки, забезпечуючи адаптивний і проактивний захист даних.

Основні компоненти системи Digital Guardian DLP

1. Клієнтський агент (Endpoint Agent).

Агенти встановлюються на кінцеві пристрої (персональні комп’ютери, ноутбуки, мобільні телефони) й виконують функції постійного моніторингу дій користувача з конфіденційними даними. Вони фіксують копіювання, переміщення, зміну або надсилання файлів і, залежно від політик, можуть застосовувати блокування, шифрування або інші запобіжні заходи.

2. Мережева частина (Network DLP).

Мережева складова Digital Guardian відповідає за контроль трафіку, що проходить через корпоративну інфраструктуру. Вона аналізує електронну пошту, інтернет-запити, передачу файлів через FTP та інші протоколи, і в разі виявлення чутливої інформації — може автоматично зупинити її передачу або попередити адміністратора.

3. Центральний сервер керування (Management Server).

Це ядро системи, яке забезпечує централізоване зберігання даних, координацію між компонентами, управління політиками та обробку інцидентів. Через сервер адміністратор може задавати правила контролю, аналізувати поведінку користувачів, формувати звіти та миттєво реагувати на виявлені порушення.

4. Сховище даних (Data Storage Protection).

Digital Guardian інтегрується з системами зберігання, такими як файлові сервери, бази даних та хмарні платформи, щоб забезпечити повний контроль доступу до інформації. Захист реалізується через шифрування, моніторинг дій з файлами та обмеження прав користувачів, що мінімізує ризик витоку або втрати даних.

2.3 Технології виявлення та запобігання витоку: Data in Use, Data in Motion, Data at Rest

Головна мета системи Digital Guardian DLP — забезпечити захист конфіденційної інформації на всіх етапах її життєвого циклу. Це означає, що контроль і політики безпеки застосовуються незалежно від того, де саме

перебувають дані — зберігаються, передаються чи обробляються користувачами [16].

На рис. 2.6 зображено три ключові стани інформації, які враховуються під час впровадження політик DLP:

- Data At Rest — інформація знаходиться в стані зберігання (на жорсткому диску, у базі даних або хмарному сховищі);
- Data In Motion — інформація передається мережею (через електронну пошту, FTP, веб-запити тощо);
- Data In Use — інформація активно використовується або змінюється на пристрої користувача (копіювання, редагування, вставка в документи, друк тощо).

Digital Guardian DLP дозволяє встановити гнучкі політики захисту для кожного з цих станів, що забезпечує безперервну безпеку даних незалежно від способу їх обробки або місця перебування.

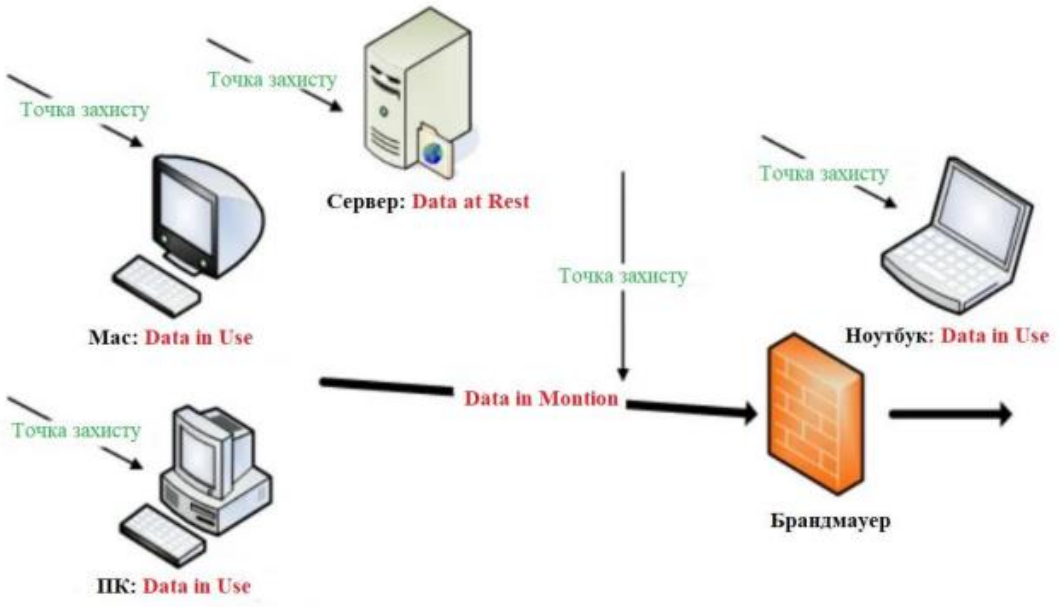

Рисунок 2.6 – Моделі захисту даних у стані зберігання, передачі та використання

У системі Digital Guardian DLP захист даних охоплює всі три основні інформаційні стани, з урахуванням особливостей кожного з них.

Data At Rest — це контроль інформації, яка зберігається у файлах, базах даних, сховищах документів чи хмарних середовищах. Digital Guardian здійснює контентне сканування для виявлення конфіденційного вмісту, наприклад номерів кредитних карток, персональних даних або фінансової звітності. У разі виявлення таких даних у неавторизованих місцях, система може автоматично виконати дію: зашифрувати, видалити файл або сповістити його власника, залежно від заданої політики.

Data In Motion — це захист інформації, що передається по мережі. Digital Guardian аналізує мережевий трафік (через проксі-сервер або в пасивному режимі) і виявляє спроби передавання конфіденційного вмісту через такі канали, як електронна пошта, миттєві повідомлення або веб-трафік. На основі централізованих політик система може блокувати або дозволяти передачу, залежно від типу контенту та ризиків.

Data In Use — це захист даних у момент їх активного використання. Digital Guardian працює на рівні кінцевих точок, відстежуючи дії користувачів із чутливою інформацією. Наприклад, система може виявити спробу перенесення конфіденційного файлу на USB-накопичувач і дозволити лише певним користувачам такі дії, або повністю їх блокувати. Також виявляються дії, пов’язані з копіюванням-вставкою, використанням даних у неавторизованих програмах або спробами шифрування для прихованого виведення файлів за межі системи.

Стан Data In Motion охоплює дані, які перебувають у процесі передачі мережею — від одного пристрою до іншого, включно з локальними мережами, інтернетом або хмарними платформами. Саме в цьому стані дані є особливо вразливими до перехоплення, змін чи несанкціонованого доступу, оскільки зловмиснику не обов’язково мати фізичний доступ до пристрою — достатньо опинитися на одному з проміжних етапів маршруту.

Digital Guardian DLP реалізує розширений контроль за трафіком, що проходить через мережу, та ідентифікує чутливу інформацію, яка може бути передана без належного захисту. Наприклад, логіни, паролі, банківські реквізити

або інша особиста інформація не повинні передаватися у відкритому вигляді. Якщо виявлено спробу такої передачі, система блокує її або застосовує шифрування відповідно до встановленої політики.

Для забезпечення надійності каналу зв'язку, Digital Guardian підтримує використання тунелів шифрування, які забезпечують збереження конфіденційності та цілісності інформації під час її переміщення. Захист даних у стані Data In Motion є ключовим елементом у стратегії інформаційної безпеки, особливо в умовах віддаленої роботи, хмарної інтеграції та високої мобільності бізнесу [17].

Схему захисту даних у русі наведено на рисунку 2.7.

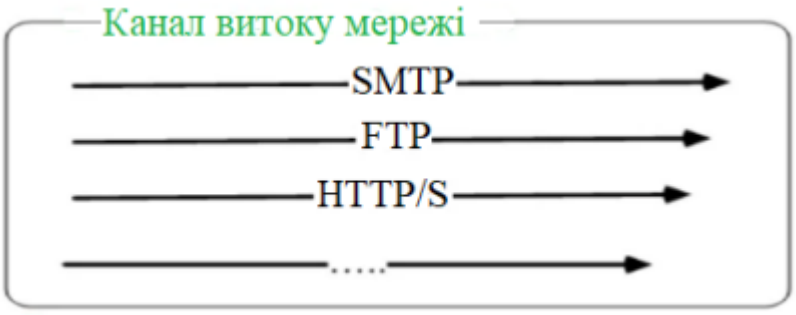

Рисунок 2.7 – Архітектура контролю даних у русі в системі DLP

Моніторинг мережі є однією з базових функцій системи Digital Guardian DLP, яка забезпечує контроль за передачею даних у реальному часі. У більшості випадків рішення DLP використовують пасивний підхід до мережевого моніторингу, що дозволяє виявляти потенційні загрози без втручання в сам трафік.

Компонент моніторингу зазвичай розгортається на порті SPAN або поряд із мережевим шлюзом, де здійснює повне захоплення пакетів, реконструює сесії користувачів і виконує глибокий аналіз вмісту в потоці. Завдяки цьому Digital Guardian здатний ідентифікувати конфіденційні дані, що передаються мережею, і миттєво застосовувати відповідні політики безпеки — наприклад, блокування передачі або генерацію інциденту.

У більшості організацій такий підхід забезпечує достатню пропускну здатність, оскільки реальна мережева активність рідко досягає рівня, який вимагає повноцінної продуктивності гігабітного Ethernet. Тому навіть у масштабних середовищах Digital Guardian може ефективно працювати без потреби у спеціалізованому обладнанні високої потужності.

Схематичне зображення принципу мережевого моніторингу наведено на рисунку 2.8.

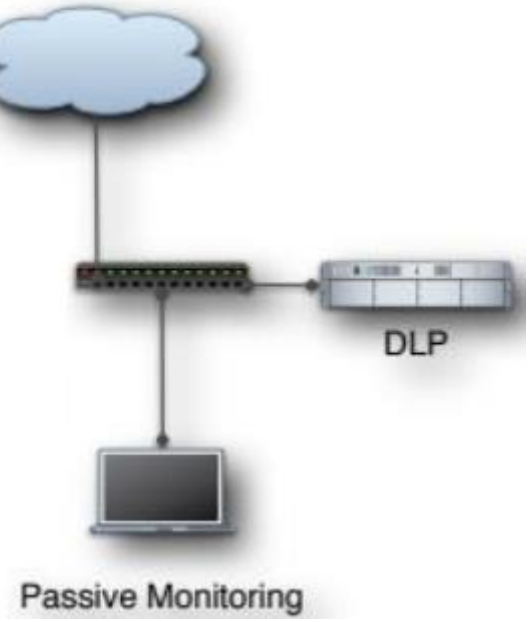

Рисунок 2.8 – Пасивний мережний моніторинг

Digital Guardian DLP — це, перш за все, інструмент для моніторингу дій користувачів і контролю обігу конфіденційної інформації, а не для аналізу загального вебтрафіку додатків. Його завдання полягає у виявленні, фільтрації та реагуванні на спроби витоку даних, пов’язаних з людським фактором, а не просто з передачею інформації через мережу.

У більшості випадків малі організації працюють із мережевим трафіком до 50 МБ/с, середні — у межах 50–200 МБ/с, а великі підприємства — до 300 МБ/с або вище, іноді досягаючи 500 МБ/с. Однак через значне навантаження, яке створює аналіз вмісту пакетів, не всі DLP-рішення виконують повне захоплення трафіку. У таких випадках компанії стикаються з вибором: або застосувати

попередню фільтрацію, втрачаючи частину нестандартного трафіку, або інвестувати в додаткові апаратні засоби з балансуванням навантаження.

Крім того, деякі DLP-продукти обмежуються аналізом трафіку лише на визначених портах або протоколах, без глибокої ідентифікації каналів зв'язку. Це створює ризик, що нестандартні способи передавання даних, зокрема підключення через незвичні порти, залишаться поза контролем. Навіть якщо система підтримує ідентифікацію каналів на основі вмісту, важливо переконатися, що ця функція активована й налаштована належним чином.

У переважній більшості випадків мережеві монітори реалізуються як універсальні сервери з попередньо встановленим ПЗ DLP. Деякі постачальники надають спеціалізовані апаратні рішення з вбудованими функціями звітності, керування робочим процесом і політиками безпеки. Проте в більшості сценаріїв основна логіка керування та звітності виноситься на окремий сервер або пристрій, що дозволяє централізувати обробку й масштабувати інфраструктуру.

Інтеграція електронної пошти є ще одним критично важливим компонентом системи Digital Guardian DLP, який забезпечує контроль за передаванням конфіденційної інформації через корпоративну пошту. Система може інтегруватися з поштовими сервісами як на локальному сервері (наприклад, Microsoft Exchange), так і в хмарному середовищі (зокрема Microsoft 365 або Gmail), щоб аналізувати вміст листів, вкладення та адреси одержувачів.

Digital Guardian здатний автоматично виявляти чутливі дані в електронних повідомленнях — наприклад, персональні дані, фінансову або медичну інформацію — та застосовувати відповідні заходи безпеки: блокування надсилання, шифрування або створення інциденту для подальшого розслідування.

Ця функція є надзвичайно важливою в контексті попередження витоків через найпоширеніший канал комунікації — електронну пошту, особливо коли мова йде про випадкове пересилання документів або помилкове введення адресата [18].

Схему інтеграції поштової системи з DLP-рішенням наведено на рисунку 2.9.

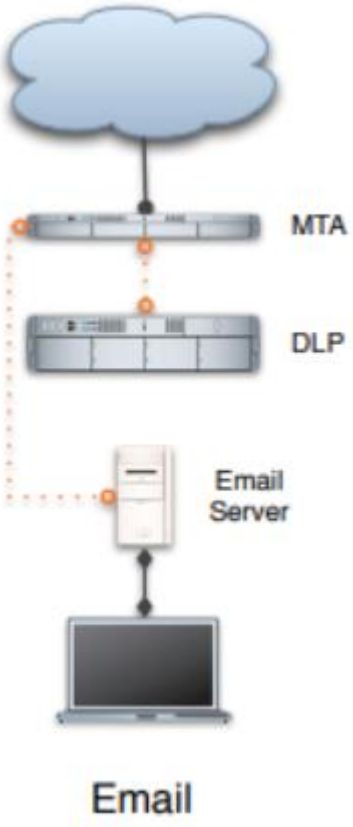

Рисунок 2.9 – Взаємодія поштового сервера з системою Digital Guardian

Оскільки електронна пошта є одним із найбільш поширених каналів для пересилання конфіденційної інформації, її інтеграція в Digital Guardian DLP надає широкі можливості для захисту, фільтрації та контролю вмісту. Завдяки тому, що електронні листи проходять етапи зберігання та передачі, система може впроваджувати карантин, шифрування, фільтрацію та інші заходи безпеки без ризику блокування синхронного трафіку в реальному часі.

Більшість DLP-рішень, зокрема Digital Guardian, вбудовують власний MTA (Mail Transfer Agent) у архітектуру продукту, що дозволяє додавати захист пошти як окремий етап у стандартний ланцюг обробки електронних повідомлень. Крім того, система може інтегруватися з провідними платформами захисту електронної пошти, підвищуючи загальний рівень безпеки й оптимізуючи продуктивність.

Однак цей підхід має обмеження: внутрішня корпоративна пошта, яка передається в межах одного поштового сервера (наприклад, Microsoft Exchange), не проходить через зовнішній MTA, і тому не завжди потрапляє під захист у реальному часі. Для повного контролю над внутрішнім поштовим трафіком необхідна глибока інтеграція з поштовими платформами (Exchange, Lotus), що рідко підтримується ринковими рішеннями. Окремі постачальники називають підтримкою внутрішньої пошти лише сканування логів або бібліотек постфактум, що не забезпечує рівня контролю, необхідного для оперативного захисту.

Фільтрація, блокування та інтеграція проксі є важливою складовою реалізації політик контролю в системі Digital Guardian DLP, особливо коли компанія переходить від пасивного моніторингу до активного захисту. Блокування трафіку — завдання складне, оскільки воно потребує точного розмежування між дозволеним і небажаним трафіком на основі аналізу вмісту в реальному часі.

Найпростішим каналом для фільтрації залишається електронна пошта: вона за своєю природою є асинхронною і має чітку структуру, що дозволяє легко інтегрувати додаткові етапи перевірки. Однак у більшості інших типів комунікацій (веб-трафік, FTP, обмін файлами, миттєві повідомлення) трафік є синхронним, тобто передається та обробляється в реальному часі. У таких випадках блокування повинне відбуватися миттєво, щоб не впливати на працездатність системи.

Існує два основні підходи до фільтрації трафіку:

1. Міст (bridge) — це система з двома мережевими інтерфейсами, яка розміщується на шляху передавання даних і виконує аналіз вмісту в реальному часі. Якщо виявлено порушення, з'єднання припиняється. Хоча метод незалежний від протоколів, він не гарантує повне блокування небажаного трафіку вчасно, тому рідко використовується в DLP-рішеннях.

2. Проксі (proxy) — більш поширений і ефективний варіант. Проксі-сервери бувають спеціалізовані для HTTP, FTP, IM тощо. Вони збирають трафік

до його передачі, що дозволяє DLP-системі глибоко аналізувати вміст і блокувати при потребі. Багато DLP-систем, зокрема Digital Guardian, інтегруються з існуючими проксі-рішеннями за допомогою протоколу ICAP, що забезпечує передачу трафіку на аналіз без додаткового обладнання.

Проксі-шлюзи також можуть перехоплювати SSL-з'єднання (за наявності зворотного проксі-сервера SSL), надаючи можливість аналізувати зашифрований трафік. Це вимагає внесення змін на кінцевих точках для обробки сповіщень про сертифікати, але значно розширює рівень контролю. Для контролю миттєвих повідомлень необхідна інтеграція з відповідним IM-проксі-сервером і підтримка конкретного протоколу [17-18].

Схематичне зображення принципів фільтрації, блокування та інтеграції проксі-серверів у DLP наведено на рисунку 2.10.

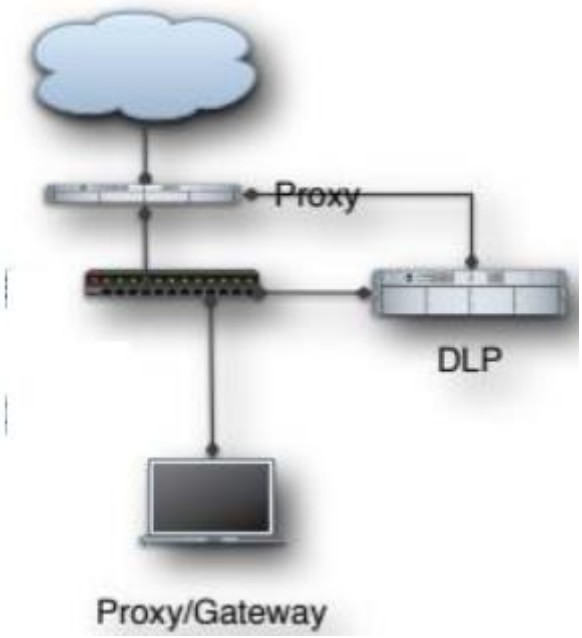

Рисунок 2.10 – Інтеграція Digital Guardian з проксі-серверами та шлюзами

Метод фільтрації TCP Poisoning (отруєння TCP) застосовується у деяких системах контролю трафіку, зокрема як один із підходів для роботи з нестандартними або не підтримуваними проксі-протоколами. У цьому методі DLP-система відстежує потік даних, і в разі виявлення порушення вводить пакет скидання TCP-з'єднання (TCP reset), аби примусово розірвати сесію.

Цей підхід технічно сумісний з усіма TCP-протоколами, однак має низку суттєвих обмежень:

– По-перше, ефективність обмежена, оскільки деякі сервіси (наприклад, поштові сервери) не припиняють спроби передавання повідомлень. Наприклад, після зупинки одного повідомлення, поштовий сервер може продовжувати повторювати спроби відправлення протягом кількох днів (наприклад, кожні 15 хвилин протягом 72 годин).

– По-друге, як і у випадку з підходом "міст", аналіз даних відбувається після того, як трафік вже почав передаватися. Це означає, що до моменту виявлення небажаного вмісту, частина даних уже могла бути витоком.

Незважаючи на ці недоліки, TCP Poisoning може бути корисним для покриття нестандартних протоколів, які складно охопити класичними проксі-рішеннями. Однак оптимальним підходом залишається використання проксі-серверів, які дозволяють перехоплювати трафік до його передачі, що забезпечує глибший аналіз і надійніше блокування.

Контроль внутрішніх мереж є технічно реалізованим у більшості сучасних систем DLP, включно з Digital Guardian, однак на практиці такий підхід застосовується переважно для електронної пошти, тоді як моніторинг іншого внутрішнього трафіку використовується значно рідше.

Причиною цього є те, що внутрішній трафік часто обходить мережеві шлюзи, які слугують основними точками фільтрації та реалізації політик DLP. Шлюзи забезпечують зручне розміщення контролю, тому їх переважно використовують для перехоплення вихідного трафіку.

Попри це, внутрішній моніторинг розглядається як перспективний напрямок з погляду вартісної ефективності, точності виявлення інцидентів і гнучкого управління політиками. Деякі постачальники DLP, зокрема й Digital Guardian, мають партнерські інтеграції або пропонують окремі рішення для моніторингу внутрішнього пересування даних. Проте для більшості організацій цей напрям не є першочерговим, оскільки потребує додаткових ресурсів і складнішої інфраструктури.

Розподілені та ієрархічні розгортання є ключовими можливостями Digital Guardian DLP, які дозволяють ефективно впроваджувати захист даних у великих та географічно розподілених організаціях. Середні, великі підприємства та навіть багато малих компаній часто мають кілька офісів, регіональних представництв і власні веб-шлюзи, тому система DLP повинна підтримувати множинні точки моніторингу.

Digital Guardian дозволяє реалізувати комбінацію таких підходів: пасивний мережевий моніторинг, проксі-контроль, інтеграція з поштовими серверами та підтримка віддалених локацій. Хоча обробку та первинний аналіз інцидентів можна делегувати на віддалені вузли, усі події централізовано передаються до головного сервера керування, де здійснюється повноцінна звітність, аудит, розслідування та архівування.

Підтримка ієрархічного розгортання дає змогу компаніям з міжнародною присутністю або великою внутрішньою структурою впроваджувати відокремлене управління політиками безпеки за регіонами, філіями чи бізнес-напрямами. Це особливо актуально для організацій, які повинні дотримуватися місцевого законодавства у сфері моніторингу персоналу й захисту даних, яке може суттєво різнитися між країнами.

Ієрархічна модель дозволяє локальним підрозділам мати власні сервери керування, які синхронізуються з центральним DLP-сервером. Такий підхід забезпечує гнучке, але узгоджене впровадження політик, дозволяючи комбінувати корпоративні, регіональні та локальні налаштування, а також налаштування звітності й робочих процесів відповідно до потреб бізнесу.

Стан ***Data at Rest*** описує ситуацію, коли дані зберігаються на носіях — таких як файлові сервери, жорсткі диски, бази даних чи хмарні сховища — але при цьому не передаються і не обробляються активно. Надійний захист у цьому стані є критично важливим, оскільки саме тут дані можуть залишатися протягом тривалого часу, і, у разі фізичного або мережевого доступу до носія, можуть стати легкою мішенню для атак.

У контексті Digital Guardian DLP, дані вважаються захищеними в стані спокою, якщо:

- вони зашифровані за допомогою криптографічно стійких алгоритмів;
- ключ шифрування не зберігається на тому ж носії, що й самі дані;
- ключ має достатню довжину і ступінь випадковості, що робить його несприйнятливим до атак словника чи грубої сили.

Такі вимоги дозволяють забезпечити, що навіть у випадку крадіжки фізичного пристрою чи несанкціонованого доступу до файлів, інформація залишиться недоступною без відповідного ключа.

Схему захисту даних у стані Data at Rest наведено на рисунку 2.11.

Рисунок 2.11 – Схема шифрування та контролю доступу до збережених даних

Існує широкий спектр технологій, які використовуються для забезпечення захисту даних у стані Data at Rest. Ці технології варіюються від шифрування носіїв до систем контролю доступу, і всі вони мають на меті унеможливити несанкціонований доступ до інформації, що зберігається на пристроях або в хмарному середовищі [19].

У системі Digital Guardian DLP ці засоби можуть бути інтегровані або працювати у взаємодії з іншими елементами безпекової інфраструктури.

На рисунку 2.12 наведено основні технології захисту інформації у стані зберігання (Data at Rest).

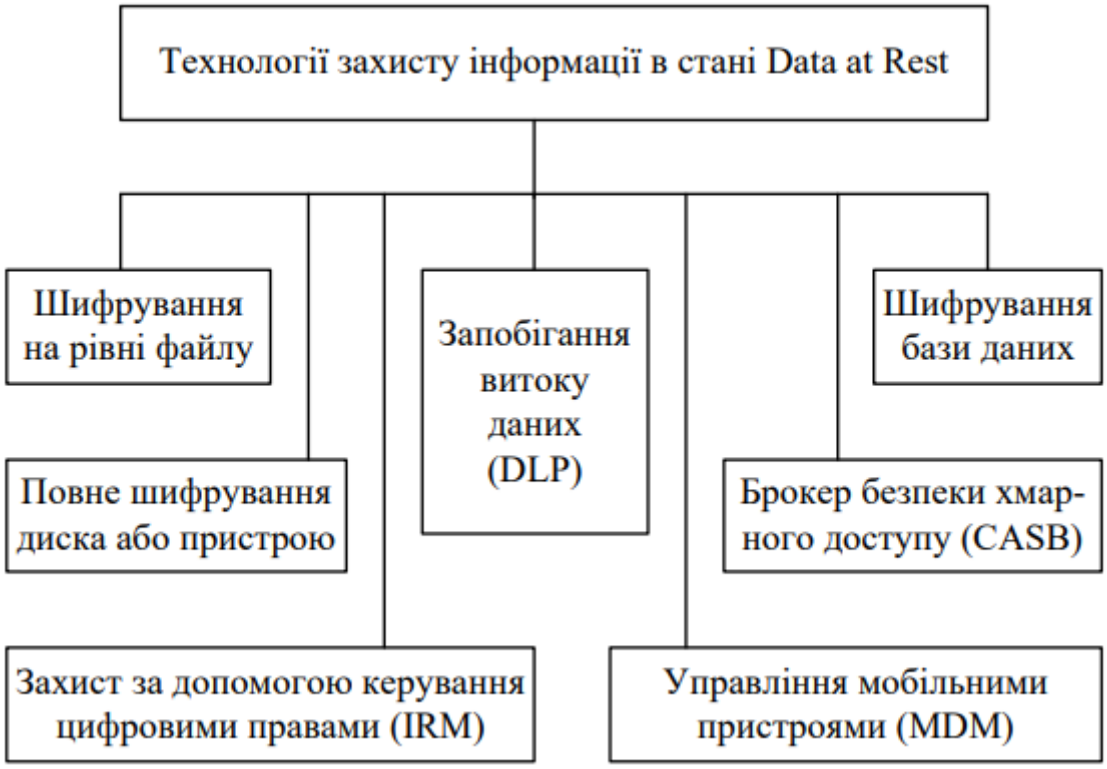

Рисунок 2.12 – Інструменти захисту інформації у Data at Rest в Digital Guardian

Для ефективного захисту даних у стані Data at Rest, існує ряд технологій, що можуть працювати окремо або в поєднанні з системами DLP, такими як Digital Guardian. Вони охоплюють як шифрування, так і контроль доступу, управління правами та мобільними пристроями. Основні з них:

1. Повне шифрування пристрою або жорсткого диска.

Дає змогу унеможливити доступ до даних у разі фізичної втрати пристрою (наприклад, ноутбука). Шифрування є прозорим для авторизованого користувача, але втрачає ефективність, якщо дані копіюються або виводяться за межі пристрою.

2. Шифрування на рівні файлу.

Дає змогу вибірково захищати окремі файли. Може бути реалізоване за допомогою симетричного або асиметричного (PGP) шифрування. Хоча воно

надає гнучкість, для обміну файлами потрібен обмін ключами, і після розшифрування файл може втратити захист.

3. Шифрування баз даних (TDE).

Реалізується в таких СУБД, як SQL Server, Oracle, і забезпечує шифрування даних та журналів у реальному часі. Забезпечує безперервну безпеку під час зберігання, але не захищає дані після їх вилучення через застосунок.

4. Керування цифровими правами (IRM / DRM).

Системи типу SealPath накладають постійний захист на файли, дозволяючи лише дозволеним користувачам відкривати або редагувати документи, не надаючи повного доступу до розшифрування. Це дозволяє зберігати контроль навіть після розповсюдження документа.

5. Управління мобільними пристроями (MDM).

Дає змогу шифрувати, обмежувати або блокувати доступ до корпоративної інформації на мобільних пристроях. Однак після того, як дані залишають пристрій (наприклад, надсилаються), вони вже не перебувають під контролем.

6. DLP-системи (у т.ч. Digital Guardian).

Можуть сканувати кінцеві точки й мережеві сховища на наявність конфіденційних даних. DLP може заблокувати доступ, перемістити або видалити файли, якщо вони не відповідають політикам. Проте втрачає контроль, коли дані виходять за межі середовища організації.

7. Брокери безпеки хмарного доступу (CASB).

Працюють з такими сервісами, як Office 365, Box, Salesforce, і дозволяють застосовувати політики DLP до даних у хмарі. Вони виявляють конфіденційні документи, можуть обмежити загальний доступ, вилучити відкриті посилання тощо. Як і DLP, діють, поки файл залишається у межах контрольованого середовища.

Рисунок 2.13 ілюструє ключові проблеми захисту інформації у стані Data at Rest, пов’язані з межами ефективності технологій, залежністю від середовища та уразливістю даних після виходу за межі контрольованих систем.

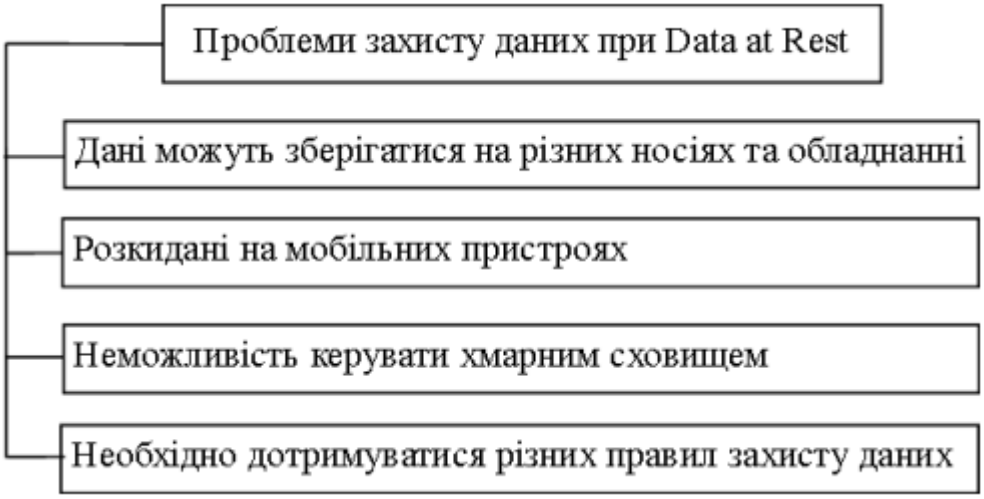

Рисунок 2.13 – Основні проблеми безпеки даних у стані Data at Rest

У реальних умовах захист даних у стані Data at Rest стикається з низкою практичних викликів, які ускладнюють повноцінне впровадження безпеки. Digital Guardian DLP дозволяє частково або повністю подолати ці обмеження, однак важливо розуміти природу основних проблем.

1. Розпорошення інформації по різних носіях.

Конфіденційні документи можуть зберігатися не лише на файлових серверах або в системах керування документами, але й на персональних комп’ютерах, USB-накопичувачах та інших пристроях. Таке розосередження ускладнює контроль і потребує постійну інвентаризацію даних.

2. Наявність копій на мобільних пристроях.

Смартфони та планшети дедалі частіше використовуються як повноцінні робочі інструменти, що містять чутливу інформацію. Проблема посилюється тим, що у багатьох випадках ці пристрої є особистими, не підконтрольними IT-відділу, і не мають корпоративних засобів захисту [19].

3. Втрата контролю в хмарних сховищах.

Більшість хмарних постачальників пропонують шифрування даних у стані спокою, однак ключі шифрування часто зберігаються у самих провайдерів, а не в компаній-користувачів. Це створює ризик втрати контролю над збереженими документами.

4. Дотримання галузевих регламентів.

Компанії в різних галузях — зокрема охорони здоров’я (HIPAA), фінансів (PCI DSS) або у межах ЄС (GDPR) — зобов’язані дотримуватися строгих вимог до захисту даних у стані зберігання, незалежно від середовища (сервер, мобільний пристрій, база даних). Порушення вимог може мати юридичні й фінансові наслідки.

Стан Data in Use стосується ситуацій, коли дані активно використовуються — переглядаються, редагуються або опрацьовуються на пристрої користувача або в робочому середовищі застосунку. У цьому стані до інформації здійснюється безпосередній доступ, а отже, навіть раніше зашифровані дані, як правило, розшифровуються для обробки, що створює додаткові ризики.

Digital Guardian DLP забезпечує захист Data in Use шляхом моніторингу дій користувача та контролю точок доступу до чутливих файлів. Це дозволяє:

- виявляти спроби несанкціонованого копіювання, переміщення або друку документів;
- блокувати вставлення конфіденційного вмісту в незахищені програми;
- фіксувати факти доступу до критично важливих даних.

У стані Data in Use дані є особливо вразливими, оскільки навіть легітимні користувачі можуть, свідомо чи ненавмисно, ініціювати витік. Наприклад, копіювання даних у буфер обміну, перенесення файлу на USB-накопичувач або вставлення в особисту електронну пошту — все це дії, які можуть бути автоматично виявлені та заблоковані засобами Digital Guardian.

На рисунку 2.14 показано загальну схему вразливостей і процесів у стані Data in Use, а рисунок 2.15 ілюструє принцип розміщення захисту на етапі до доступу до вмісту — тобто ще до того, як дані стануть відкритими для взаємодії.

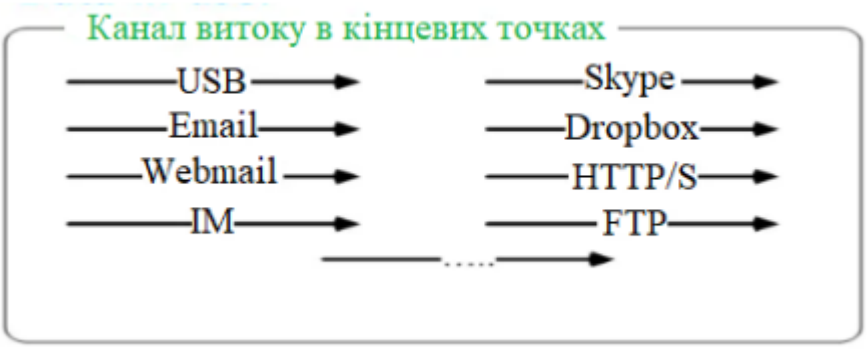

Рисунок 2.14 – Захист даних у процесі використання (Data in Use)

Рисунок 2.15 – Механізми керування до відкриття чутливої інформації

Захист у стані Data in Use є найскладнішим, оскільки дані в цей момент розшифровані та доступні для взаємодії, що створює потенціал для ненавмисного чи зловмисного витоку. Сучасні DLP-рішення, такі як Digital Guardian, впроваджують багаторівневий контроль на цьому етапі.

1. Інструменти ідентифікації та аутентифікації.

Перший рівень захисту — перевірка, чи є користувач тим, за кого себе видає. Важливу роль відіграє двофакторна аутентифікація (2FA), яка суттєво знижує ризик доступу сторонніх осіб у випадку крадіжки облікових даних.

2. Умовний доступ і моделі на основі ролей (RBAC).

Дозволяють обмежити доступ до даних на основі ролі, місцезнаходження, IP-адреси або інших атрибутів. Проте, як тільки користувач отримав доступ, традиційні методи не можуть обмежити, що саме він робить з даними.

3. Захист цифрових прав (IRM / DRM).

IRM дозволяє не лише надати доступ, а й контролювати дії після доступу — наприклад, заборонити друк, редагування або збереження копій. Це особливо ефективно, коли доступ потрібен лише для перегляду. Захист переміщується разом із файлом, незалежно від того, чи він в хмарі, чи вже завантажений на пристрій користувача.

4. Проблеми Data in Use.

Навіть при обмеженнях дій, візуалізація документа в програмі завжди залишає ризик — наприклад, створення знімка екрана. Це частково можна пом’якшити за допомогою динамічних водяних знаків. Крім того, спільні платформи, які обмежують завантаження або редагування, зручні лише для перегляду, але обмежені у функціональності.

5. Недоліки хмарних платформ.

Навіть якщо документ захищений, під час доступу він розшифровується на стороні хмарного провайдера, що потенційно відкриває доступ до вмісту навіть без участі користувача. Це критично для даних, що підпадають під регуляції (GDPR, HIPAA тощо).

6. Шифрування в оперативній пам’яті.

Теоретично можливо забезпечити захист у RAM, але це складно реалізувати без втрати продуктивності. Найбільш реалістичний і ефективний підхід — використання IRM, що поєднує шифрування, контроль дозволів і ідентифікацію користувача [17-19].

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ OPENVPN-СЕРВЕРА ДЛЯ ЗАХИСТУ МЕРЕЖІ

3.1 Встановлення та налаштування агента Digital Guardian на кінцевій точці

З метою реалізації системи контролю витоку даних у рамках дипломного проєкту було здійснено розгортання агента Digital Guardian (DG Agent) на тестовій робочій станції під керуванням Windows. Один із способів перевірки, чи працює агент, полягає у визначенні його наявності на файловій системі та/або в активних процесах операційної системи.

Кроки перевірки наявності агента Digital Guardian:

1. Запуск командного рядка від імені адміністратора. Оскільки встановлення агента потребує привілеїв адміністратора, усі перевірки слід виконувати з відповідним рівнем доступу.

2. Перевірка наявності директорії встановлення. За замовчуванням агент встановлюється у папку: C:\Program Files\DGAgent

– Якщо директорія існує, це свідчить про те, що агент було встановлено або принаймні розпочато його інсталяцію.

– Якщо директорія відсутня, існує два варіанти: агент ніколи не встановлювався або встановлення завершилось із помилкою.

3. Індикація роботи агента через обмеження створення папки.

Якщо агент працює в режимі Stealth Mode, то директорія C:\Program Files\DGAgent буде прихована або захищена.

– Спроба створити цю папку вручну за допомогою команди: mkdir DGAgent

призведе до повідомлення "Access is denied". Це означає, що агент дійсно запущений і працює.

4. Аналіз процесів у диспетчері задач.

При відсутності стелс-режиму можна перевірити наявність наступних процесів у системі:

– DgAgent.exe
– DgService.exe
– DgWip.exe
– DgUpdate.exe

Якщо будь-який із них активний — агент запущений.

5. Додаткова перевірка логів встановлення.

У разі підозри на помилку інсталяції перевіряється наявність файлів:

– C:\Windows\DGAgentInstall.log
– C:\Windows\DGAgentUninstall.log\

Аналіз часу створення та вмісту логів дозволяє встановити, чи інсталяція завершилася успішно [20].

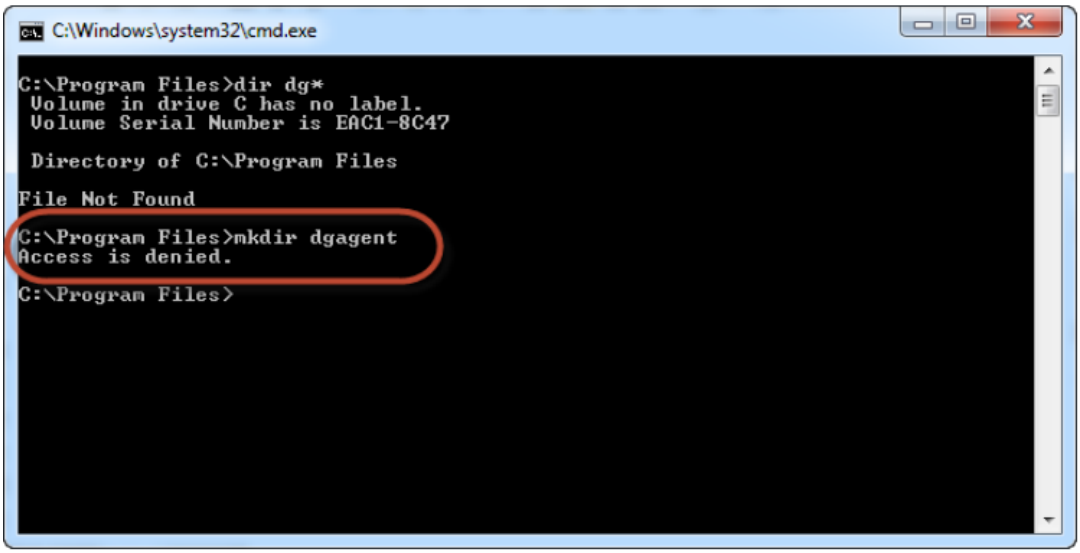

Рисунок 3.1 – Неможливість створення каталогу DGAgent у системному розділі, що вказує на активну роботу агента Digital Guardian у стелс-режимі

Перевірка зв'язку агента Digital Guardian з центральним сервером

Для забезпечення повноцінного функціонування агента Digital Guardian, необхідно перевірити можливість встановлення з'єднання між агентом та сервером DGCOMM. Це дозволяє підтвердити, що передача даних, логів і

команд між кінцевою точкою та сервером здійснюється безперешкодно.

Умови виконання перевірки:

- Доступ до машини з агентом (локально або через віддалене підключення).
- Наявність адміністративних прав на системі.
- Можливість використання браузера (у нашому випадку – Internet Explorer).

Послідовність дій:

1. Авторизуємося на машині з агентом Digital Guardian.
2. Відкриваємо браузер Internet Explorer.
3. У рядок адреси вводимо тестову URL-адресу, замінивши номер інстансу на актуальний:
   https://<номер_DGMC>dgcommp01.msp.digitalguardian.com/dgcomm/services.aspx
   Наприклад:
   https://dgcommp01.msp.digitalguardian.com/dgcomm/services.aspx
4. Результат перевірки:

Якщо вікно завантажується з порожнім вмістом (білий екран без помилок) — це означає, що агент успішно підключається до сервера Digital Guardian, і проблем з мережею чи сертифікатами не виявлено.

5. Якщо ж браузер повертає повідомлення про помилку підключення (HTTP error / connection timeout / certificate error) — потрібно перевірити:
   - Наявність виходу в Інтернет.
   - Проксі або мережеві фільтри.
   - Системні сертифікати.
   - Фаєрвол або антивірусні обмеження.

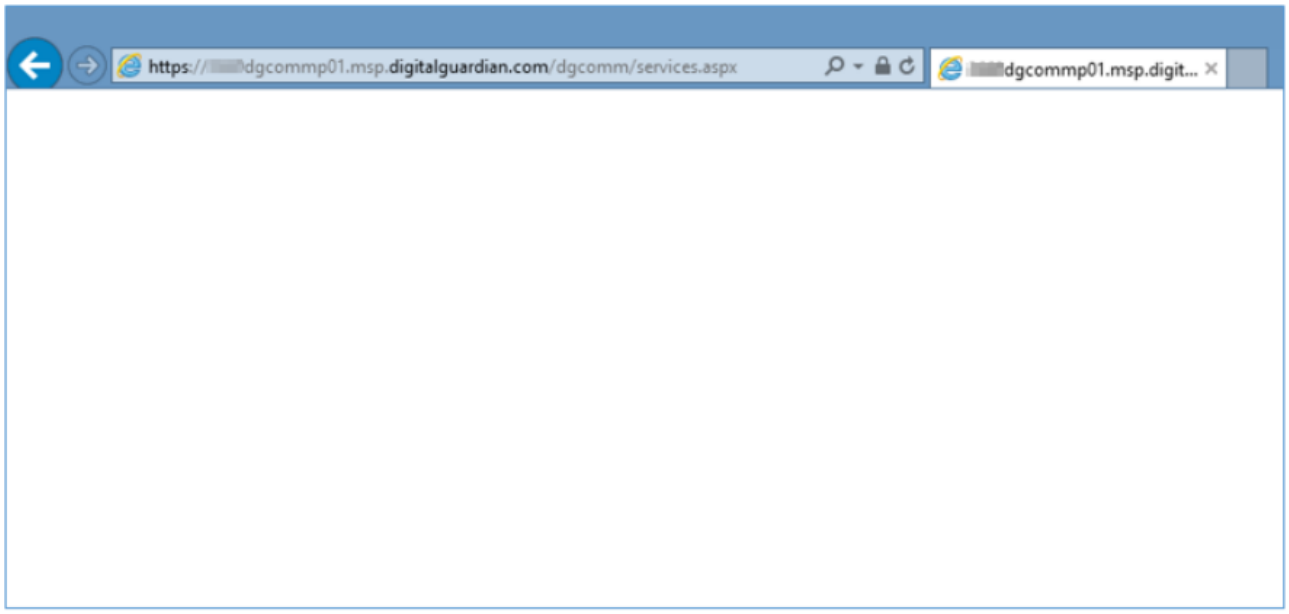

Рисунок 3.2 – Успішна перевірка з'єднання агента Digital Guardian із сервером

DGCOMM через веб-браузер (Браузер Internet Explorer відкриває URL https://dgcommp01.msp.digitalguardian.com/dgcomm/services.aspx і повертає порожню сторінку – що свідчить про нормальну комунікацію з сервером.)

Наступним етапом перевірки є тестування комунікації агента з сервером DGCOMM через браузер [21].

1. Відкриваємо Internet Explorer на машині з агентом.
2. Переходимо за URL:

https://<YourDGMC#>dgcommp01.msp.digitalguardian.com/dgcomm/services.aspx

Якщо відкрилася порожня сторінка, це означає, що агент успішно підключений до сервера.

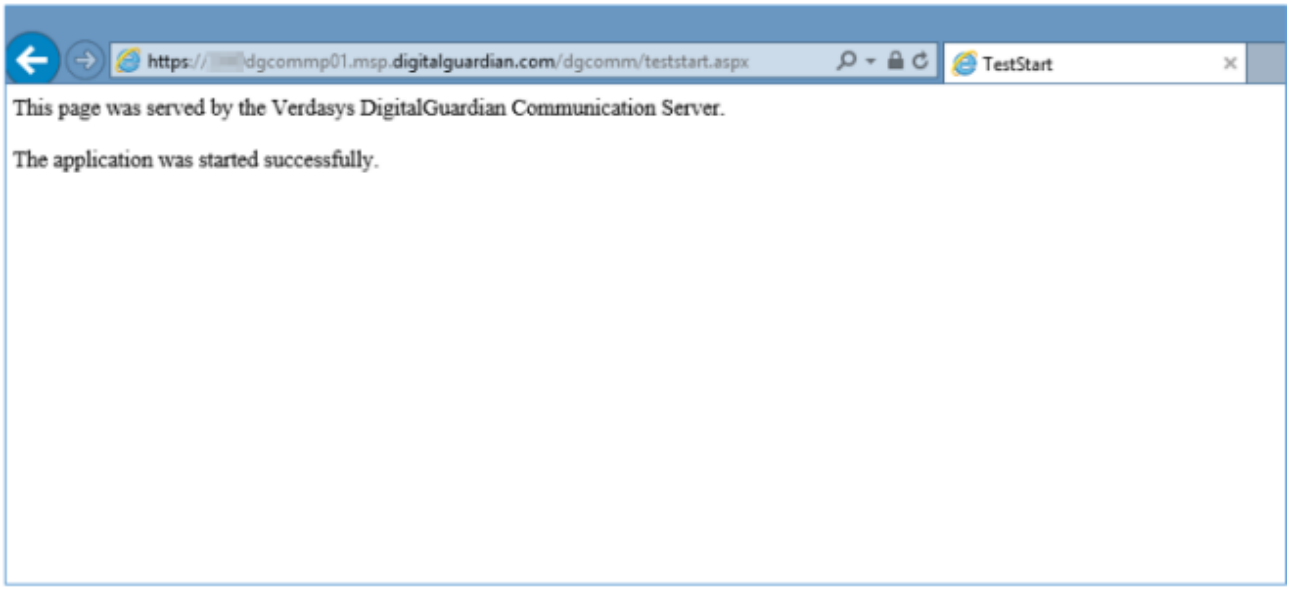

Рисунок 3.2 – Перевірка з’єднання агента з сервером Digital Guardian (порожня сторінка означає успішне з’єднання)

У процесі усунення несправностей або перевірки впливу агента на систему може знадобитися тимчасово завершити або запустити DG Agent із панелі керування DGMC.

Умови:

- Необхідно мати повний доступ (Full Control) до розділів:
  - System > Computers > Terminate Agent
  - System > Computers > Start Agent

Послідовність дій:

1. Увійти до DGMC (Digital Guardian Management Console).
2. Перейти в розділ System > Computers.
3. У списку знайти цільову машину з агентом.
4. Обрати дію:
   - Terminate Agent – для зупинки агента.
   - Start Agent – для повторного запуску.

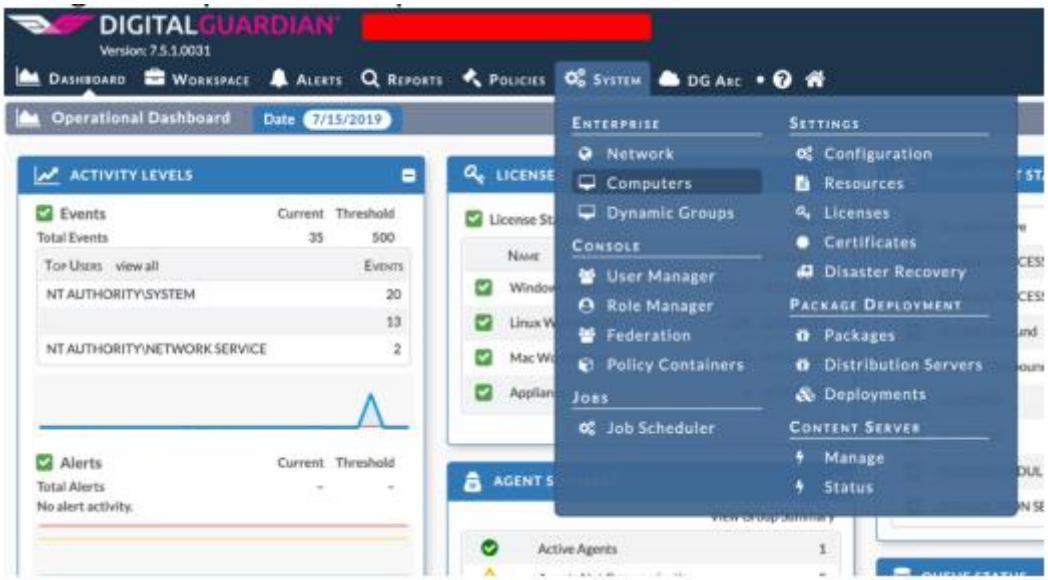

Рисунок 3.4 – Доступ до керування комп’ютерами через меню “System > Computers” в DGMC

Після відкриття розділу System > Computers у DGMC необхідно знайти конкретний пристрій, на якому потрібно завершити або запустити агент.

Дії:

1. Натискаємо на вкладку All Agents.
2. У полі Search By Computer вводимо ім’я хоста цільового комп’ютера.
3. Після знаходження потрібної системи натискаємо дію Terminate або Start, залежно від мети.

Цей крок дозволяє точково взаємодіяти з агентами на різних кінцевих точках, зокрема під час усунення несправностей або перевірки статусу агента [21].

Рисунок 3.5 – Інтерфейс пошуку комп’ютера за ім’ям хоста в DGMC для

керування агентами

Після того як потрібний комп’ютер знайдено за hostname у DGMC:

1. Обираємо цільову систему в списку.
2. Натискаємо на кнопку “Actions” (іконка з трьома горизонтальними лініями).
3. Вибираємо пункт Run Agent Commands.
4. Зі списку обираємо відповідну дію:

– Terminate Agent – для примусової зупинки агента.

– Start Agent – для запуску агента на обраному пристрої.

Цей інструмент є корисним для віддаленого управління агентами без потреби фізичного доступу до кінцевої точки.

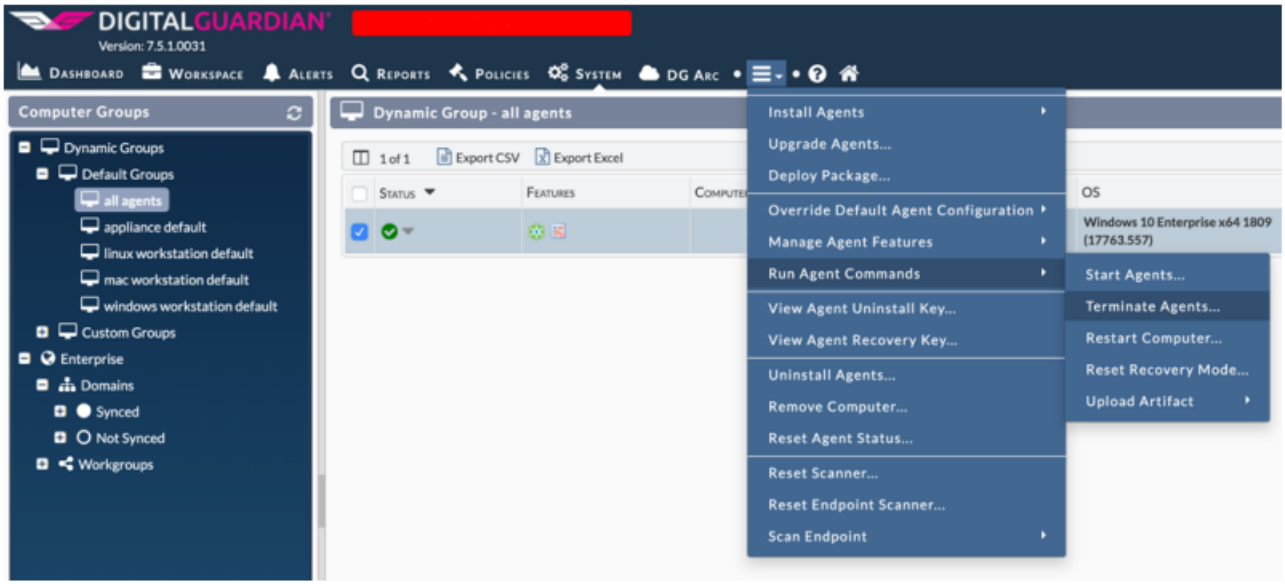

Рисунок 3.6 – Виконання команд запуску або завершення агента через меню “Run Agent Commands” в DGMC

Після вибору дії Start або Terminate Agent, команда буде поставлена в чергу на виконання. Агент отримає її під час наступного звернення до сервера (за замовчуванням кожні 30 хвилин).

Перевірка запланованих дій:

1. У таблиці комп’ютерів натискаємо на ім’я хоста обраної системи.

2. У вікні профілю пристрою відкриваємо вкладку Pending Tasks.

3. Тут відображаються всі очікуючі команди, які ще не були виконані агентом.

Цей механізм дозволяє відстежувати статус керуючих дій і переконатися, що команда на запуск або зупинку агента не була втрачена.

У випадку системного збою (BSOD) або аварійного завершення програми важливо швидко з’ясувати, який компонент викликав помилку. Для цього використовується аналіз дампу пам’яті через утиліту WinDBG, що входить до складу Windows SDK.

Умови [22]:

- Адміністративний доступ до системи.
- Отриманий дамп пам’яті після збою.
- Встановлений WinDBG (x64) (рекомендується вибрати лише цей компонент при інсталяції Windows 10 SDK).

Кроки:

1. Запускаємо WinDBG (x64).
2. В меню обираємо File > Open Crash Dump…
3. Відкриваємо файл .dmp, збережений після збою.
4. Після завантаження натискаємо !analyze -v для запуску розширеного аналізу.

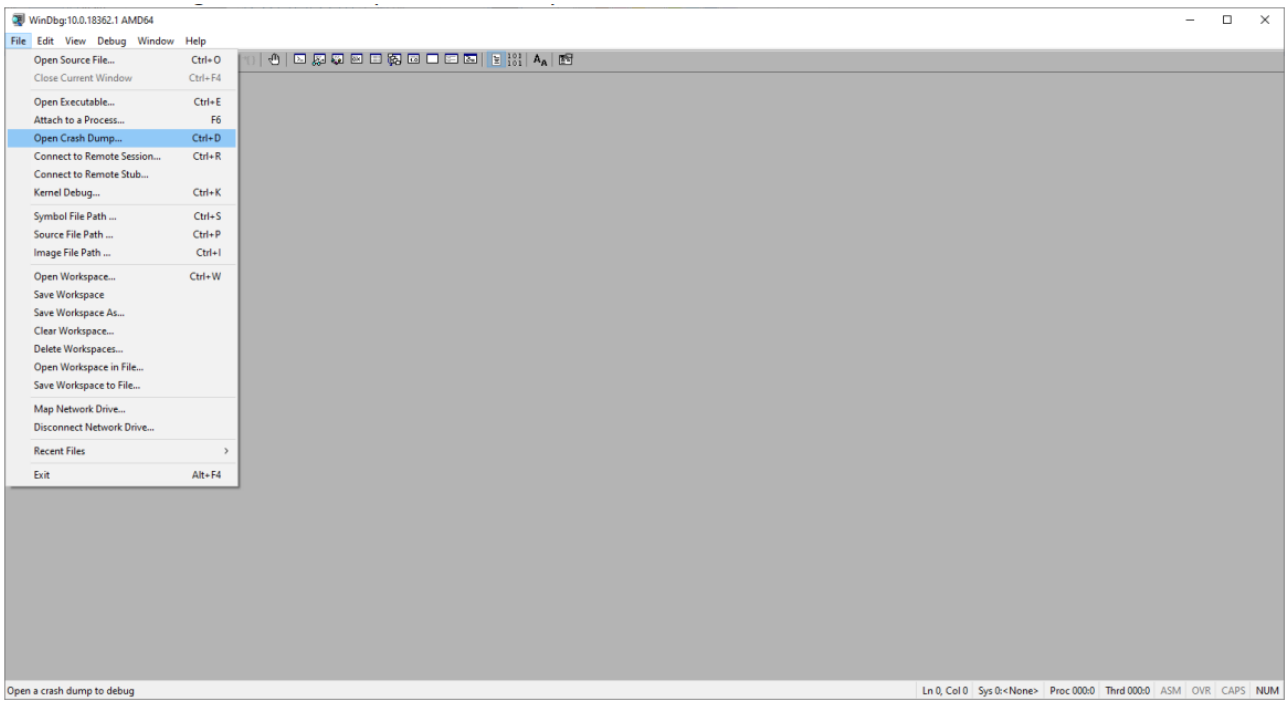

Рисунок 3.7 – Відкриття дампу пам’яті в WinDBG через пункт “File > Open Crash Dump...”

Після натискання File > Open Crash Dump... відкривається провідник файлів.

Подальші дії:

1. Перейдемо до каталогу, де збережено файл дампу пам’яті (наприклад, C:\Windows\MEMORY.DMP або .dmp з каталогу програми).
2. Виділимо відповідний файл і натиснемо "Open".

Файл буде завантажено в середовище WinDBG, після чого можна перейти до аналізу вмісту.

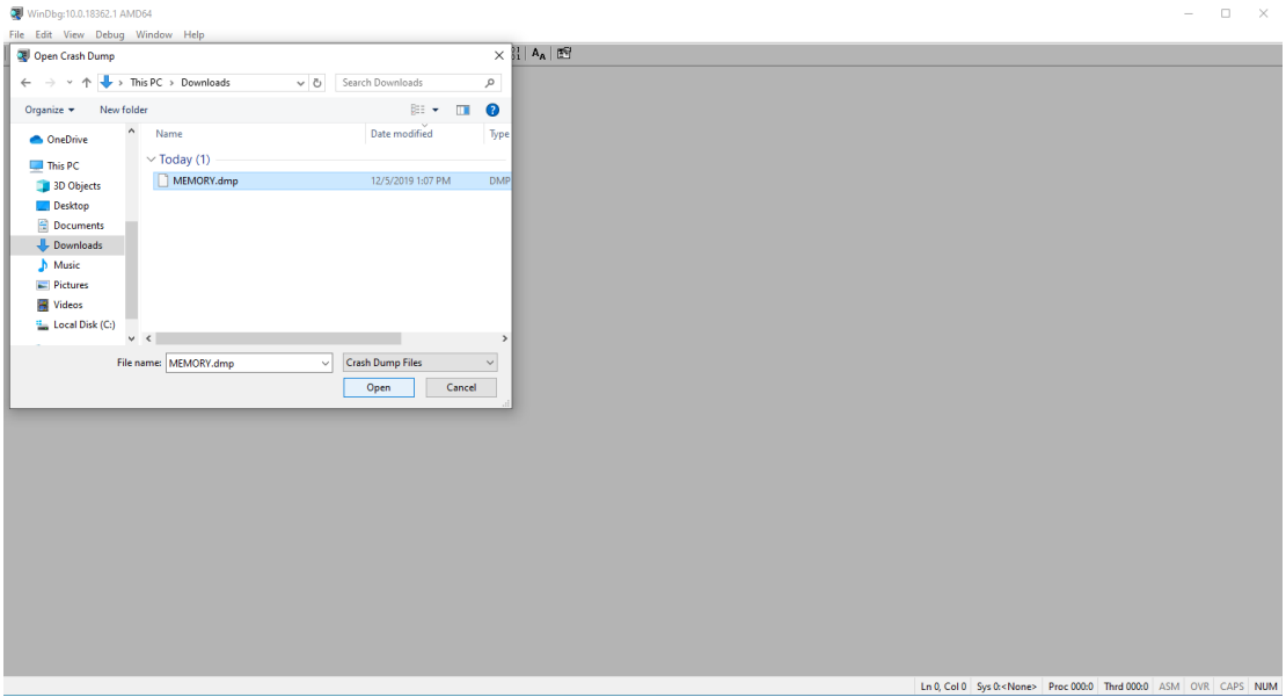

Рисунок 3.8 – Вибір файлу дампу пам’яті (MEMORY.dmp) для відкриття в WinDBG

WinDBG автоматично покаже ім’я модуля, що викликав збій, а також виробника, адресу помилки та код зупинки. Це дозволяє встановити, чи пов’язаний збій із агентом Digital Guardian чи іншим стороннім компонентом.

Після завантаження дампу пам’яті в середовищі WinDBG слід виконати команду аналізу [22]:

Кроки:

1. У вікні дампу натискаємо на гіперпосилання !analyze -v або
2. Вручну вводимо команду в нижньому полі введення:

   !analyze -v

– WinDBG почне обробку даних. У нижньому лівому куті може з’явитися позначка “busy”, що означає, що аналіз ще триває.

– По завершенні буде показано розширений звіт із вказівкою на ймовірний модуль, що спричинив збій, код помилки, адреси пам’яті та іншу корисну інформацію для діагностики.

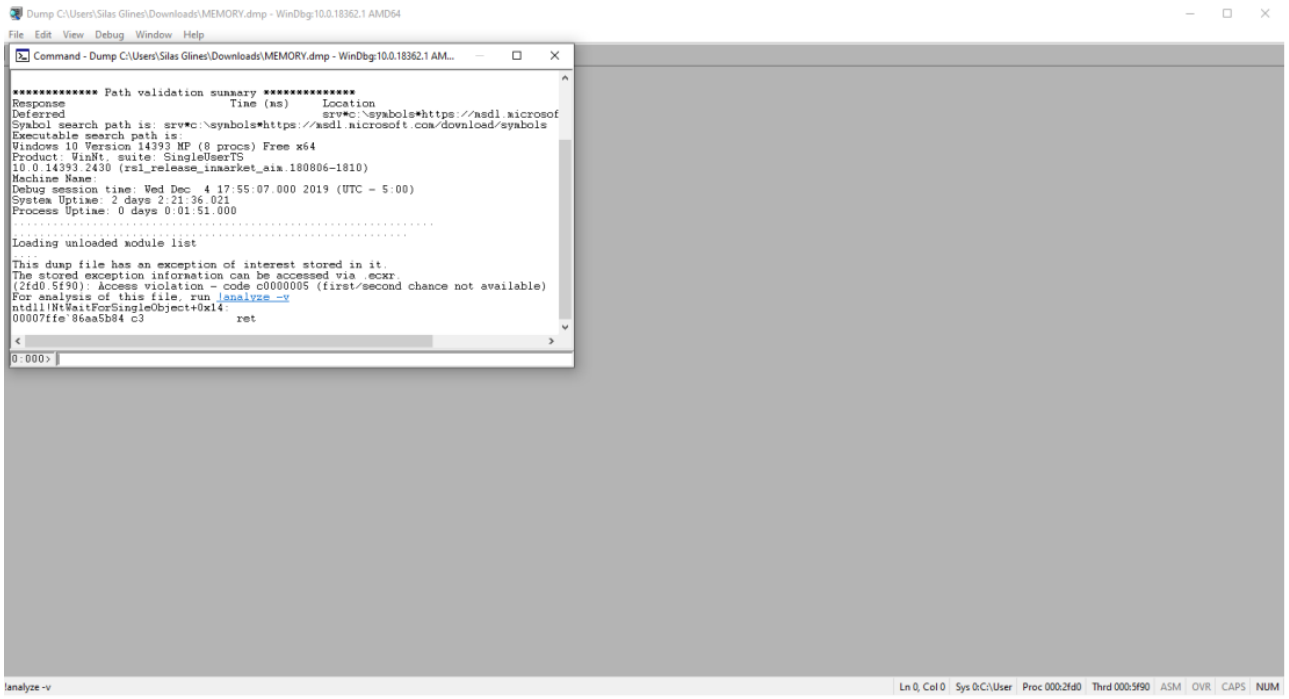

Рисунок 3.9 – Результат виконання команди “!analyze -v” у WinDBG для розширеного аналізу дампу пам’яті

Після завершення аналізу в WinDBG прокручуємо вивід у вікні дампу вниз до секції MODULE_NAME.

Кроки:

1. Знаходимо рядок MODULE_NAME – він вказує на модуль, що, за версією Windows, викликав збій.
2. Натискаємо на гіперпосилання з назвою модуля – це дозволить побачити детальну інформацію про нього, включаючи:

– Виробника (Company Name),

– Шлях до файлу,

– Адресу завантаження,

– Симптоми (якщо були).

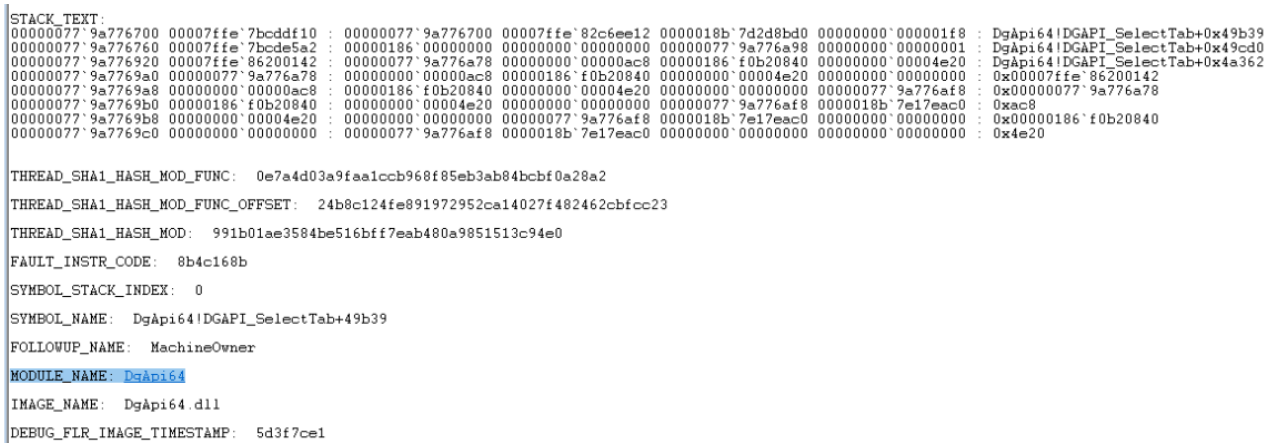

Рисунок 3.10 – Визначення модуля, що спричинив збій системи (MODULE_NAME: Dgapi64)

У нижній частині виводу WinDBG, після визначення імені модуля, звертаємо увагу на поле CompanyName.

Рисунок 3.11 – Визначення постачальника модуля, що спричинив збій системи

Web Inspection Proxy (WIP) — це власна технологія, розроблена компанією Digital Guardian, яка реалізується у вигляді проксі-сервера на локальній машині

користувача. Вона дозволяє перехоплювати та аналізувати вхідний і вихідний мережевий трафік безпосередньо на кінцевій точці. Завдяки цьому забезпечується повний контроль і прозорість мережевих операцій, що дозволяє ефективно застосовувати політики безпеки та виявляти потенційно небезпечні дії в реальному часі [23].

3.2 Управління політиками та контроль витоку даних через DGMC

Під час розгортання та тестування DLP-рішення Digital Guardian ми виконуємо перевірку роботи компонента Web Inspection Proxy (WIP). Щоб переконатися, чи не викликає він збої в роботі системи, ми тимчасово вимикаємо або знову запускаємо WIP на вибраній кінцевій точці.

Для цього:

1. Підключаємось до DGMC (Digital Guardian Management Console) з обліковим записом, який має повні права на розділ System > Computers.
2. У верхньому меню інтерфейсу обираємо вкладку System, після чого відкриваємо пункт Computers.
3. У полі Search by Computer вводимо ім’я хосту комп’ютера, на якому необхідно виконати дію, і натискаємо Enter.
4. У знайденому результаті переходимо до меню дій (іконка з трьома горизонтальними смужками), обираємо Run Agent Commands, а далі – залежно від завдання – Start Web Inspection Proxy або Terminate Web Inspection Proxy.
5. Після цього команда потрапляє в чергу і буде автоматично виконана під час наступної синхронізації агента з сервером (типово – кожні 30 хвилин).

Рисунок 3.12 – Перехід до керування комп’ютерами у DGMC

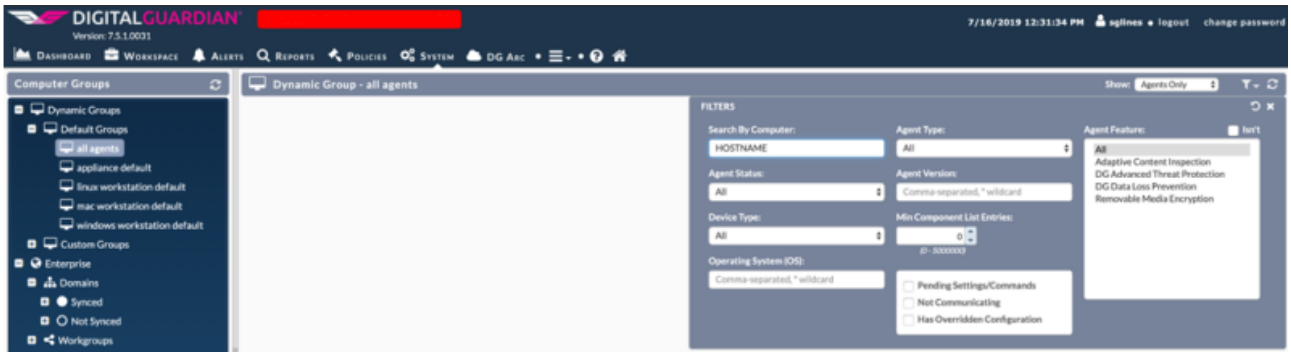

Рисунок 3.13 – Пошук комп’ютера для керування агентом у DGMC за іменем хоста

Для зміни параметрів роботи агента Digital Guardian на окремому комп’ютері необхідно перевизначити стандартну конфігурацію. Це виконується через спеціальне меню в DGMC.

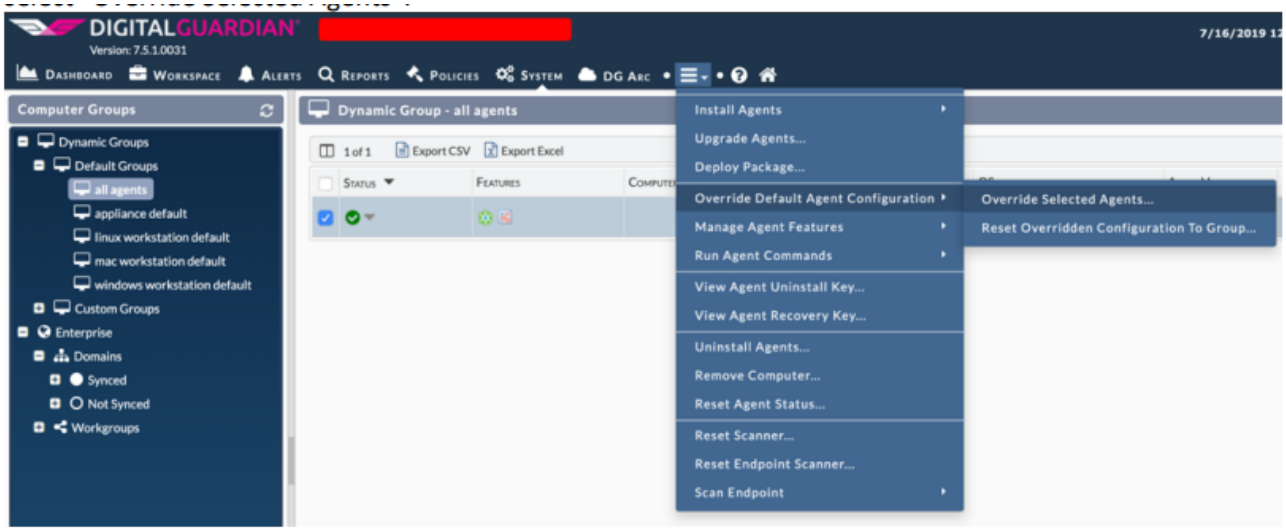

Рисунок 3.14 – Виклик меню для перевизначення конфігурації агента Digital Guardian

На етапі зміни конфігурації агента після кількох переходів у вікні налаштувань потрібно дійти до розділу Browser Settings. Саме тут можна керувати параметрами Web Inspection Proxy (WIP).

Щоб вимкнути WIP на цільовій системі:

- У розділі Disable Web Inspection Proxy встановлюємо галочки навпроти всіх опцій.

Це дозволяє тимчасово відключити веб-проксі для подальшого тестування чи усунення несправностей [23].

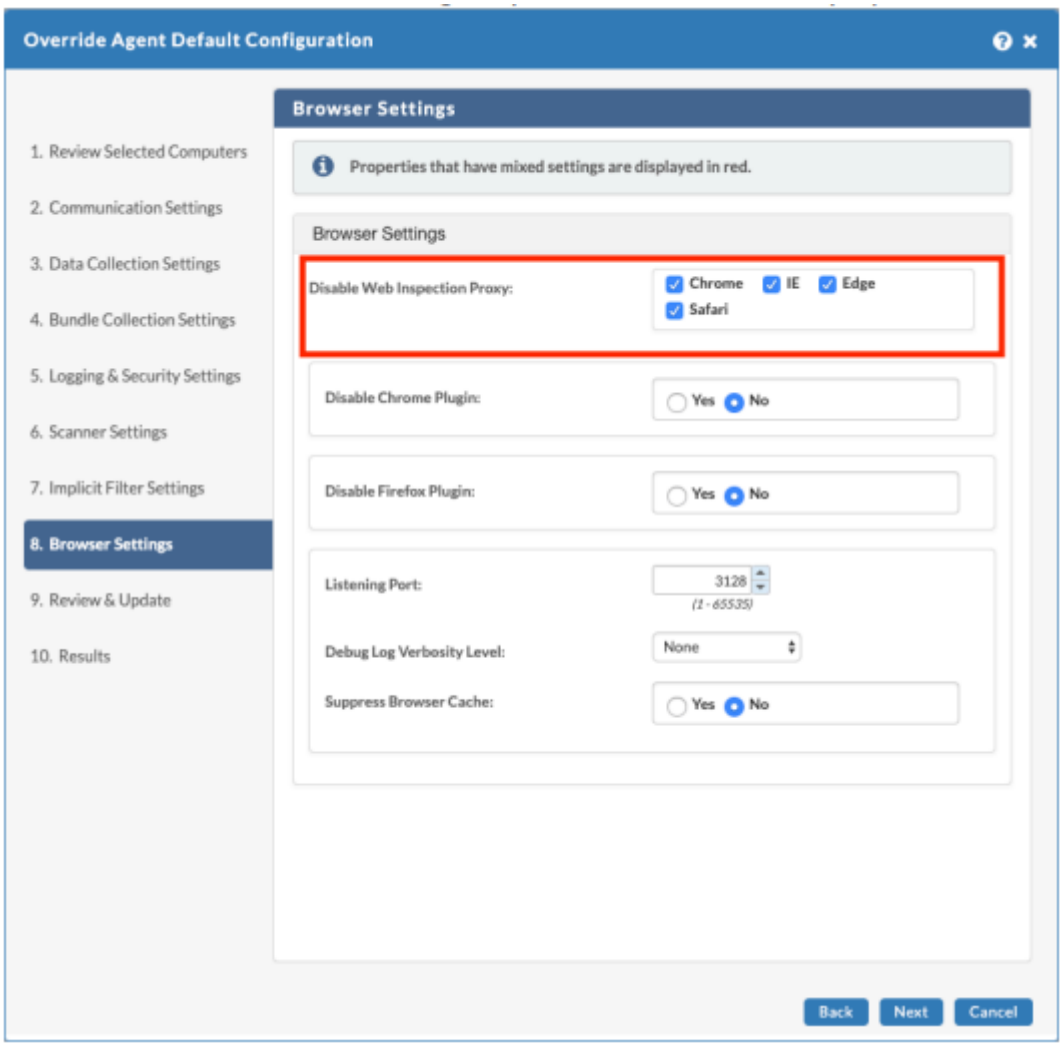

Рисунок 3.15 – Вимкнення Web Inspection Proxy (WIP) у налаштуваннях агента Digital Guardian

Щоб повторно активувати компонент Web Inspection Proxy (WIP) на цільовій системі, у вікні налаштувань агента необхідно зняти позначки біля всіх браузерів у пункті “Disable Web Inspection Proxy”. Після цього декілька разів натискаємо “Next” та завершуємо процес, натиснувши “Update”.

Команда буде поставлена в чергу та виконана агентом під час наступного звернення до сервера (типово кожні 30 хвилин). Перевірити статус виконання можна у вкладці “Pending Tasks”, натиснувши на ім’я хосту у колонці “Computer” [23].

3.3 Тестування роботи агента та аналіз ефективності виявлення загроз

Перед впровадженням змін у конфігурацію або ресурсні файли агентів у продуктивному середовищі доцільно протестувати ці зміни на обмеженій кількості систем. Такий підхід дозволяє переконатися, що модифікації дійсно вирішують поставлену проблему та не спричиняють побічних наслідків у роботі агентів.

Для реалізації тестування виконаємо наступну послідовність дій:

1. Увійдемо до DGMC, використовуючи облікові дані з відповідними правами доступу. Необхідно мати:

- повний контроль до розділів *System > Dynamic Groups*, *System > Resource Files*, *System > Job Scheduler*;
- права на перегляд до *System > Computers*.

2. Перейдемо до розділу System > Computers, де переглянемо доступні системи для тестування та виберемо необхідні.

3. Створимо нові конфігураційні та ресурсні файли, які відповідають запланованим змінам. Їх буде застосовано лише у межах тестової групи.

4. Сформуємо динамічну тестову групу, до якої буде додано обраних агентів. Це дозволить ізолювати вплив змін на основну інфраструктуру.

5. Призначимо створені конфігурації через механізм *Job Scheduler*, що дасть змогу керовано розгортати зміни та фіксувати результати впровадження.

6. Проаналізуємо поведінку агентів після застосування нових налаштувань. У разі відсутності помилок або негативних наслідків – зміни можуть бути масштабовані на всю систему [24].

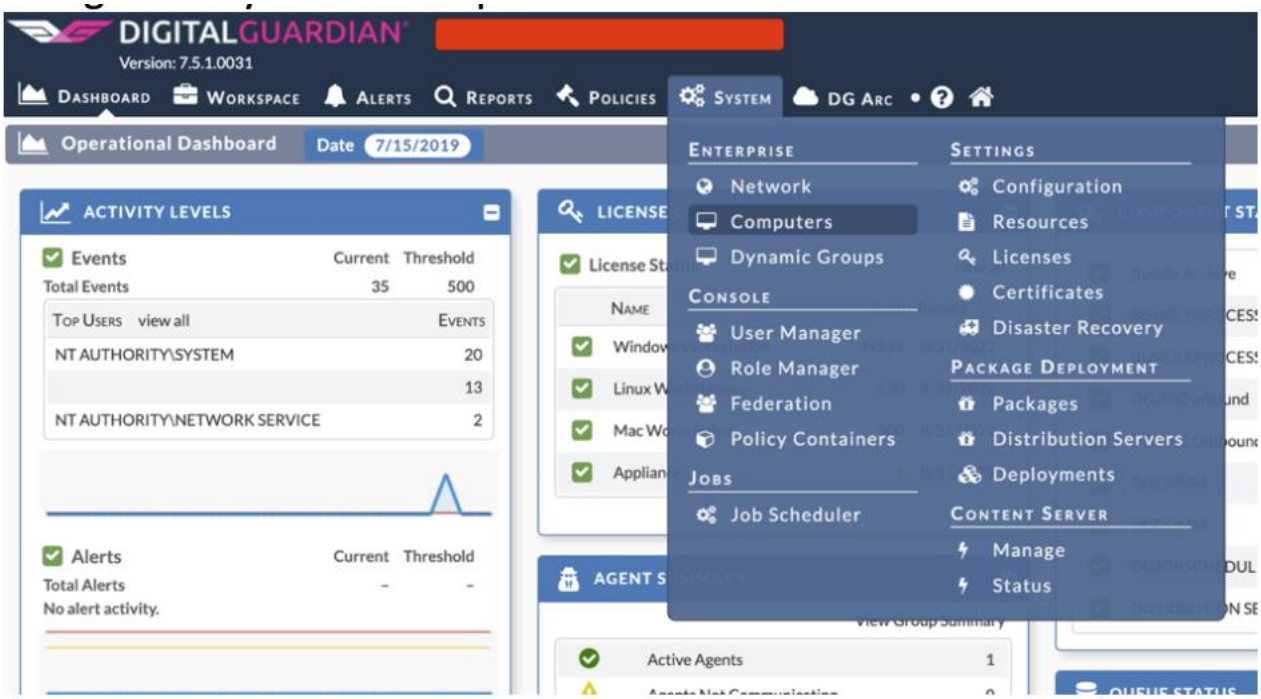

Рисунок 3.16 – Перехід до вкладки System > Computers у DGMC для керування агентами

Після переходу до розділу System > Computers продовжимо з ідентифікації цільового агента для тестування:

7. Клікнемо на пункт All Agents, щоб відкрити повний список агентів, що наразі підключені до системи.

8. Здійснимо пошук необхідної системи за її hostname, ввівши значення у поле Search By Computer. Це дозволить оперативно знайти конкретний пристрій, на якому планується протестувати нову конфігурацію або ресурсний файл.

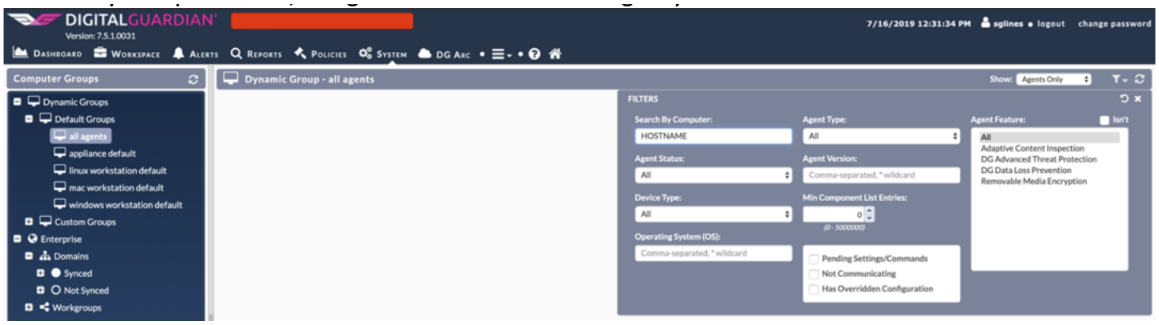

Рисунок 3.17 – Інтерфейс пошуку цільової системи за hostname у групі All Agents

9. Обираємо у списку агентів систему, на якій планується тестування, натиснувши на її hostname.

10. Перейдемо до вікна Agent Status, де відображається детальна інформація про поточний стан агента.

11. Відкриємо вкладку Resources, щоб переглянути всі конфігураційні та ресурсні файли, які наразі застосовані до цього агента. Тут слід занотувати назву конфігураційного або ресурсного файлу, на якому будуть проводитися зміни.

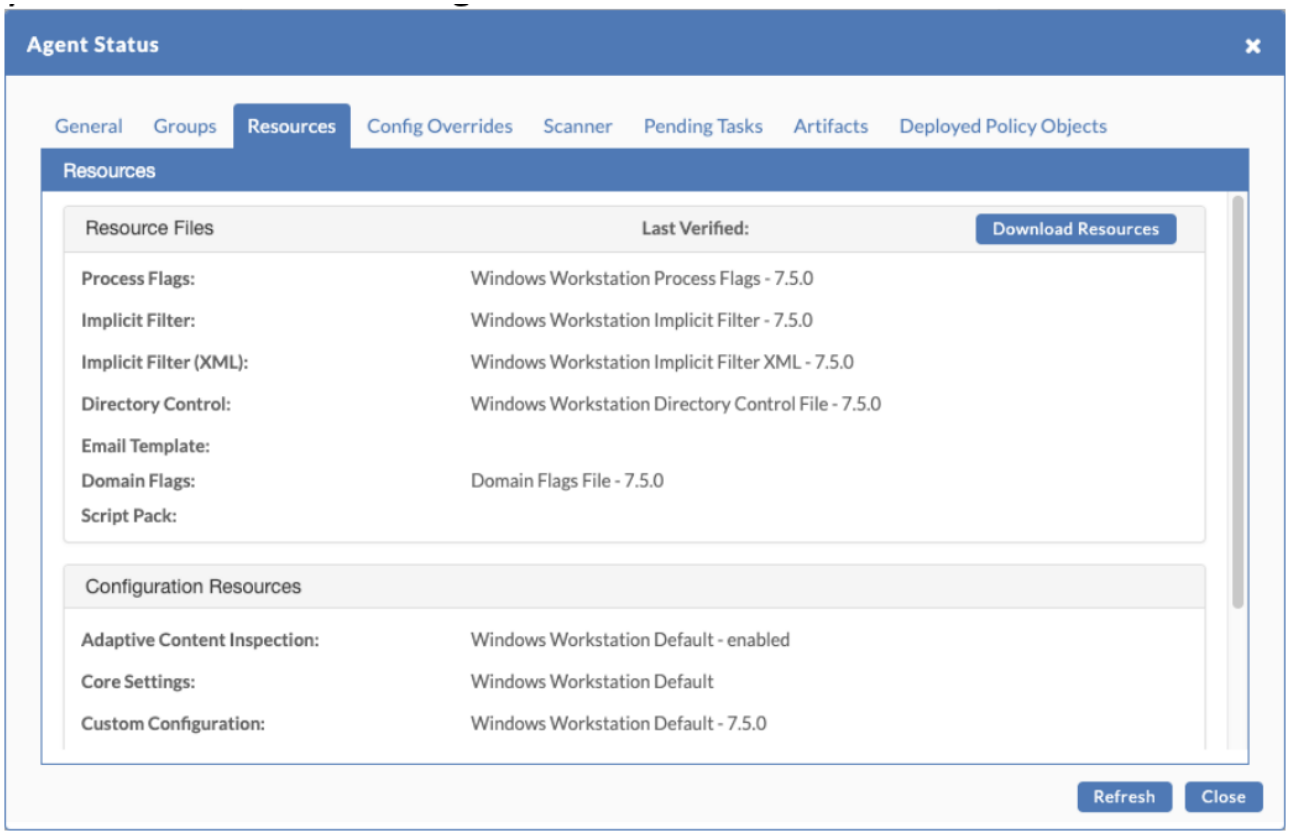

Рисунок 3.18 – Перегляд поточного набору ресурсів та конфігурацій для вибраного агента у вкладці Resources

12. Повернемося до головного меню System та перейдемо у розділ Resources, де здійснюється управління всіма доступними конфігураційними й ресурсними файлами.

13. У лівій панелі оберемо категорію ресурсів, до якої належить файл, що використовується агентом. Його назву було визначено на попередньому етапі (див. п. 11) [25].

14. Знайшовши потрібний файл, клікнемо на кнопку Clone Resource (іконка у вигляді двох аркушів), щоб створити копію ресурсу для тестування змін без впливу на основний файл.

15. Назвемо створений файл відповідно до внутрішньої угоди іменування:
<Платформа агента> <Тип файлу ресурсу> – <Версія агента> <Короткий опис проблеми> – Test.
Наприклад: Windows Workstation Directory Control File – 7.5.0 Timeout Adjustment – Test.

У випадку, якщо було відкрито кейс у службі підтримки Digital Guardian, назва може бути у форматі:
Windows Workstation Directory Control File – 7.5.0 Case 123456 Timeout Adjustment.

16. Заповнимо поле "Description", додавши коротке пояснення призначення даного тестового ресурсу, наприклад: *“Тестове оновлення для перевірки зміни таймаутів з'єднання в агента версії 7.5.0”*.

17. Внесемо усі необхідні зміни до вмісту конфігураційного або ресурсного файлу згідно з вимогами тестування.

18. Збережемо файл, натиснувши іконку Save у правому верхньому куті інтерфейсу.

19. Знайдемо щойно створений ресурс у загальному списку та встановимо його пріоритетність на рівні “1” за допомогою кнопки “Move Entry To Top Of List” (іконка зі стрілкою вгору). Це забезпечить першочергове застосування даного ресурсу агентом під час тестування.

Створення тестової динамічної групи

Для ізольованого тестування змін у конфігураційних та ресурсних файлах доцільно використовувати окрему динамічну групу. Це дозволяє не впливати на роботу агентів у продуктивному середовищі.

– Увійдемо до системи DGMC з обліковим записом, що має права на

створення та зміну динамічних груп.

– Перейдемо у розділ System > Dynamic Groups, який містить перелік наявних груп та дозволяє створювати нові.

Рисунок 3.20 – Перехід до розділу Dynamic Groups через головне меню системи DGMC

– Відкриємо меню Actions (іконка з трьома горизонтальними смужками) у правій частині інтерфейсу керування динамічними групами.
– Оберемо пункт Create Dynamic Group, після чого — Dynamic Machine Group…. Ця опція дозволяє створити нову динамічну групу на основі заданих критеріїв (наприклад, за назвою хоста, IP-адресою, версією агента тощо).

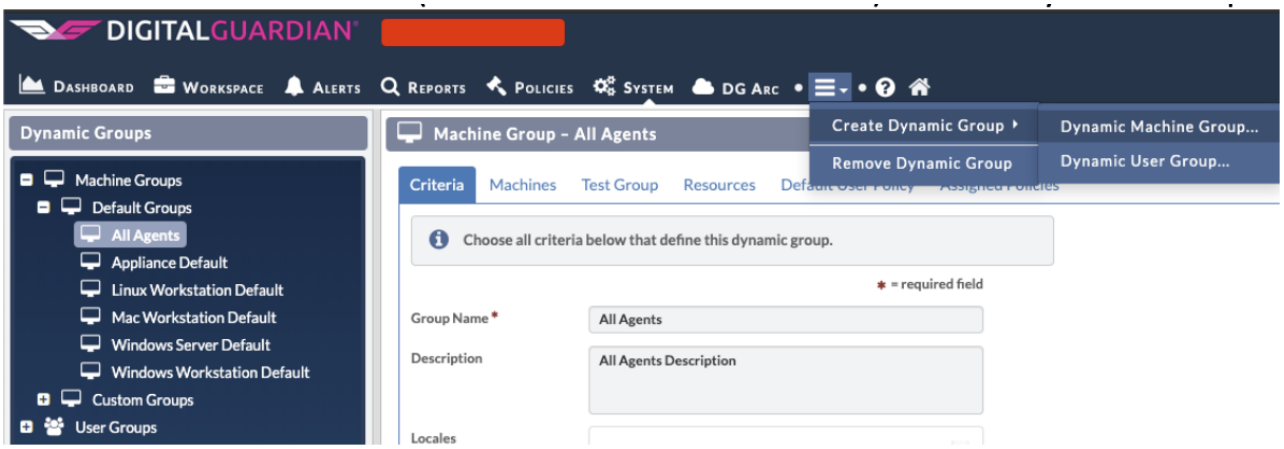

Рисунок 3.21 – Створення нової динамічної групи через меню Actions

– Натиснемо кнопку Next у першому вікні створення динамічної групи для переходу до етапу вибору систем.’
– У полі "Included Machine Names" введемо hostname тієї системи, на якій планується тестування змін у конфігурації чи ресурсах. Якщо на момент створення групи hostname ще не визначено — тимчасово використовуємо значення "PLACEHOLDER".
– Продовжимо натискати Next, доки не перейдемо до останнього вікна під назвою Test and Save Group.
– Вкажемо назву нової динамічної групи відповідно до внутрішнього стандарту іменування: <Платформа агента> – <Версія агента> <Короткий опис проблеми> – Test. Наприклад: Windows Workstation – 7.5.0 Timeout Adjustment – Test. У разі наявності відкритого звернення до технічної підтримки DG, назву групи слід оформити у форматі: Case 123456 Timeout Adjustment.
– У полі “Description” коротко опишемо призначення створюваної групи, наприклад: “Група створена для тестування конфігураційного файлу з оновленими тайм-аутами обробки запитів на агентах версії 7.5.0” [25].

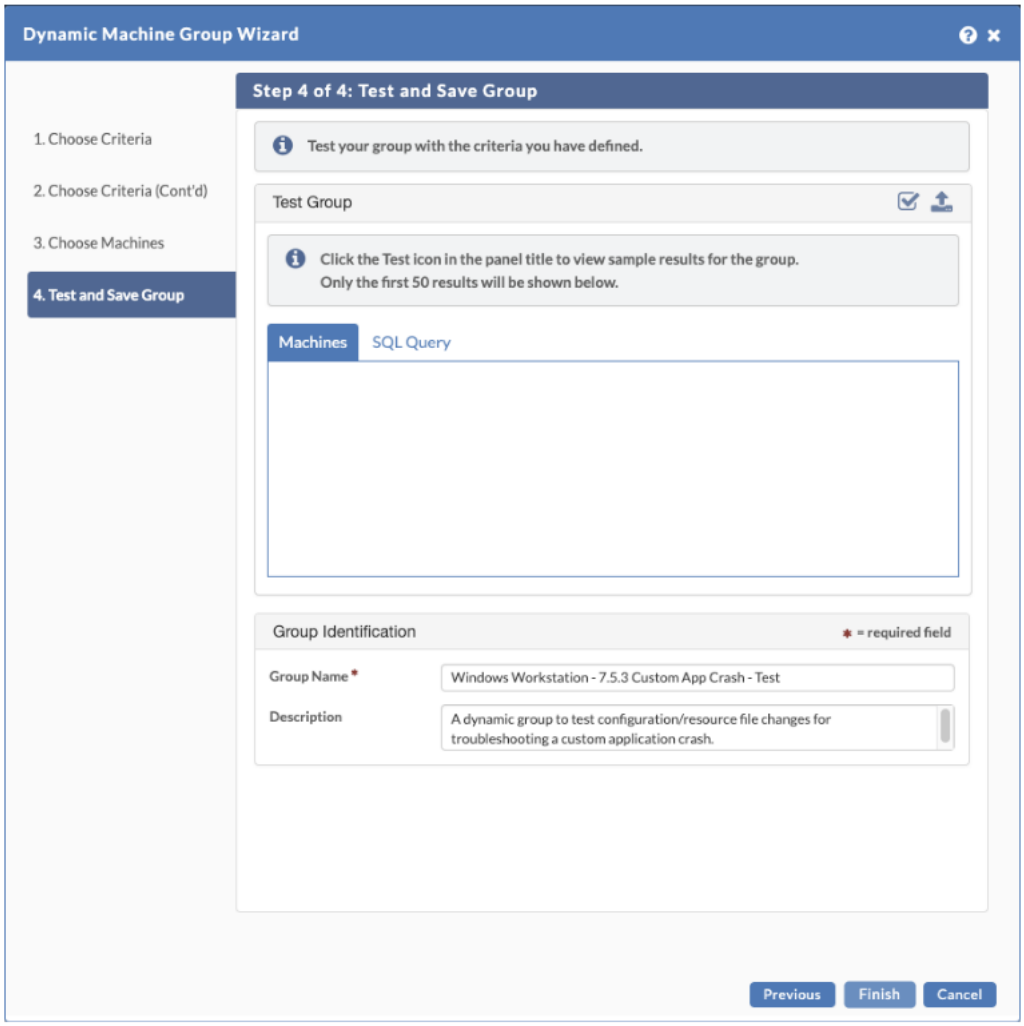

Рисунок 3.22 – Фінальний етап створення динамічної групи у вікні Test and Save Group

– Завершимо створення тестової динамічної групи, натиснувши кнопку Finish.
– Виберемо щойно створену групу зі списку динамічних груп і перейдемо до вкладки Resources, де виконується призначення конфігураційних та ресурсних файлів.
– Скористаємося випадаючими списками для того, щоб призначити раніше створений тестовий файл конфігурації або ресурсу, який був сформований на першому етапі (див. розділ "Створення тестового конфігураційного/ресурсного файлу").
– Залишимо всі інші поля у значенні "None", щоб уникнути призначення непотрібних або конфліктних параметрів.

– Натиснемо кнопку Save у верхньому правому куті інтерфейсу, щоб зберегти зміни.

Це завершальний етап підготовки агента до тестування. Після застосування тестового ресурсу група систем отримає відповідні конфігураційні оновлення, що дозволяє перевірити їхню ефективність і безпечність у контрольованому середовищі [25].

У результаті виконання усіх етапів — від створення тестового ресурсного файлу до його прив’язки до спеціально сформованої динамічної групи — було успішно проведено тестування налаштувань агента. Застосований конфігураційний файл не спричинив помилок або небажаних побічних ефектів, що свідчить про правильність внесених змін.

Агент перейшов у стабільний робочий стан, всі функції залишаються доступними, що дозволяє вважати тестове оновлення успішним і готовим до масштабування у продуктивному середовищі.

ВИСНОВКИ

1. Аналіз сучасного стану захисту конфіденційної інформації в організаціях.

У роботі було встановлено, що малі та середні підприємства є особливо вразливими до витоку конфіденційної інформації через обмежені ресурси та недостатній рівень кіберзахисту. Виявлено ключові загрози, пов’язані як із зовнішніми атаками, так і з внутрішніми порушеннями, що підтверджує необхідність впровадження спеціалізованих рішень типу DLP.

2. Вивчення вимог міжнародних стандартів.

Було досліджено рекомендації ISO/IEC 27001, NIST та регламенту GDPR щодо забезпечення захисту даних. Встановлено, що DLP-системи, зокрема Digital Guardian, здатні забезпечити відповідність цим вимогам за рахунок контролю обробки персональних даних, ведення журналів подій і впровадження політик безпеки.

3. Дослідження архітектури та функціонування DLP-систем.

Опрацьовано структуру, компоненти та принципи роботи DLP-систем, включаючи моніторинг Data in Use, Data in Motion, Data at Rest. Здійснено порівняльний аналіз основних рішень ринку (Symantec, McAfee, Forcepoint), що дозволило обґрунтувати вибір Digital Guardian для подальшої практичної реалізації.

4. Практичне розгортання агента Digital Guardian.

Виконано встановлення агента Digital Guardian на кінцеву точку, налаштовано політики безпеки через DGMC, реалізовано механізми моніторингу та фіксації інцидентів. Проведено тестування системи, яке засвідчило ефективність блокування витоку конфіденційної інформації через зовнішні пристрої, хмарні сервіси та мережеві канали.

5. Розробка рекомендацій для малого та середнього бізнесу.

На основі проведеного дослідження сформовано практичні рекомендації щодо впровадження DLP-системи в умовах обмеженого бюджету, включаючи

етапи впровадження, пріоритетні політики, адаптацію під внутрішні процеси та оптимізацію витрат на ліцензування і підтримку.

В процесі виконання кваліфікаційної роботи було розроблено покрокову методику безпечного внесення змін до DLP-агента, яка може бути використана адміністраторами інформаційної безпеки під час розгортання та підтримки систем захисту даних на підприємстві. Результати роботи можуть бути застосовані у практичній діяльності IT-відділів та служб ІБ, що впроваджують або вже експлуатують систему Digital Guardian.

ПЕРЕЛІК ПОСИЛАНЬ

1. Contributor T. Top 10 Types of Information Security Threats for IT Teams | TechTarget. Security. URL: https://www.techtarget.com/searchsecurity/feature/Top-10- types-of-information-security-threats-for-IT-teams (date of access 07.05.2025).

2. Ways to Effectively Prevent Data Leakage. SecurityScorecard. URL: https://securityscorecard.com/blog/ways-to-prevent-a-data-leakage/ (date of access: 07.05.2025).

3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 07.05.2025).

4. Кондратенко М. Система запобігання витоку інформації на підприємстві : Дипломна робота "Бакалавра". Київ, 2021. 56 с.

5. What Is DLP and How Does It Work? | Trellix. Trellix | Revolutionary Threat Detection and Response. URL: https://www.trellix.com/security-awareness/data- protection/how-data-loss-prevention-dlp-technology-works/ (date of access: 07.05.2025).

6. Boehm A. What is Data Loss Prevention (DLP)? [Guide] - CrowdStrike. crowdstrike.com. URL: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/ (date of access: 07.05.2025).

7. What is DLP? Data Loss Prevention, Meaning & Definition. Netskope. URL: https://www.netskope.com/security-defined/what-is-data-loss-prevention-dlp (date of access: 07.05.2025).

8. DLP Systems: Models, Architecture and Algorithms. Share & Discover Presentations | SlideShare. URL: https://www.slideshare.net/liwei_ren/dlp-systems-models-architecture-and-algorithms (date of access: 07.05.2025).

9. Understanding and Selecting a Data Loss Prevention Solution [Електронний ресурс] // The SANS Institute. – 2020. – Режим доступу до ресурсу: https://securosis.com/assets/library/publications/DLP-Whitepaper.pdf.

10. Security Guide [Електронний ресурс] // Fedora. – 2020. – Режим

доступу до ресурсу: https://jfearn.fedorapeople.org/fdocs/en-US/Fedora/20/html/Security_Guide/Security_Guide-Encryption-Data_in_Motion.html.

11. Cooper S. 13 Best Data Loss Prevention Software Tools [Електронний ресурс] / STEPHEN COOPER // Comparitech. – 2021. – Режим доступу до ресурсу: https://www.comparitech.com/data-privacy-management/data-loss- prevention-tools-software/.

12. BEST Data Loss Prevention Software DLP Solutions In 2022 [Електронний ресурс] // Software Testing Help. – 2022. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/data-loss-prevention-software/.

13. Software Deployment [Електронний ресурс] // Sumo Logic. – 2020. – Режим доступу до ресурсу: https://www.sumologic.com/glossary/software-deployment/.

14. What is Free Trial? [Електронний ресурс] // Chargebee. – 2020. – Режим доступу до ресурсу: https://www.chargebee.com/resources/glossaries/what-is-free- trial/.

15. Software Integration [Електронний ресурс] // Snaplogi. – 2020. – Режим доступу до ресурсу: https://www.snaplogic.com/glossary/software-integration#:~:text=Software%20integration%20is%20the%20process,including%20cloud%2Dbased%20data%20storage.

16. Digital Guardian. Endpoint Technical Support Guidebook for Windows. Version 2006. – June 2020. – 130 p. [PDF-документ із методикою налаштування, тестування та діагностики агента DG]

17. Digital Guardian. Management Console User's Guide. – [Офіційна документація Digital Guardian]. URL: https://support.digitalguardian.com/s/article/Management-Console-User-s-Guide (дата звернення: 09.05.2025).

18. Digital Guardian. Security Application Exclusions – Best Practices. – Digital Guardian Knowledge Base. URL: https://support.digitalguardian.com/s/article/Security-Application-Exclusions (дата звернення: 09.05.2025).

19. Microsoft Docs. WinDbg Preview – Windows Debugger. – Microsoft Learn. URL: https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/ (дата звернення: 09.05.2025).

20. Microsoft Docs. Sysinternals Process Monitor – Troubleshooting and Monitoring Tool. – Microsoft Learn. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon (дата звернення: 09.05.2025).

21. Forrester Research. The Forrester Wave™: Data Loss Prevention, Q3 2021. – Forrester, 2021. URL: https://www.forrester.com/report/The-Forrester-Wave-Data-Loss-Prevention-Q3-2021/RES163330 (дата звернення: 09.05.2025).

22. Gartner. Magic Quadrant for Enterprise Data Loss Prevention. – Gartner, 2023. URL: https://www.gartner.com/en/documents/4019540 (дата звернення: 09.05.2025).

23. ENISA. Guidelines on Data Protection Engineering. – European Union Agency for Cybersecurity, 2021. URL: https://www.enisa.europa.eu/publications/guidelines-on-data-protection-engineering (дата звернення: 09.05.2025).

24. OWASP Foundation. OWASP Cheat Sheet: Data Protection. – Open Web Application Security Project. URL: https://cheatsheetseries.owasp.org/cheatsheets/Data_Protection_Cheat_Sheet.html (дата звернення: 09.05.2025).

25. NIST. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) – NIST Special Publication 800-122. – National Institute of Standards and Technology, 2010. URL: https://csrc.nist.gov/publications/detail/sp/800-122/final (дата звернення: 09.05.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ