НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) **інформаційних технологій**

УДК 004.492

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету (Директор ННІ)	**Завідувач кафедри**
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
(назва факультету (ННІ))	(назва факультету (ННІ))
/ Болбот І.М., д.т.н, проф. /	/ Касаткін Д.Ю., д.п.н., доцент /
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2024 р.	«___»_____2024 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему Дослідження технології управління інцидентами інформаційної безпеки з використанням можливостей DLP-систем

Спеціальність 123 «Комп'ютерна інженерія»
(код і назва)

Освітня програма Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми

д.п.н., професор		Мамченко С.М.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Керівник магістерської кваліфікаційної роботи

д.п.н., доцент		Касаткін Д.Ю.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Виконав _____ Ляшук В.С.
(підпис) (ПІБ студента)

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних систем, мереж та кібербезпеки

д.п.н., доцент _____ Касаткін Д.Ю.
(науковий ступінь, вчене звання) (підпис) (ПІБ)
"____" _____ 20____ року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ
Ляшуку Віталію Сергійовичу
(прізвище, ім'я, по батькові)

Спеціальність 123 «Комп'ютерна інженерія»
(код і назва)

Освітня програма Комп'ютерні системи захисту інформації
(назва)

Орієнтація освітньої програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської роботи: Дослідження технології управління інцидентами інформаційної безпеки з використанням можливостей DLP-систем

затверджена наказом ректора НУБіП України від "___" 20 р. № ____

Термін подання завершеної роботи на кафедру _____
(рік, місяць, число)

Вихідні дані до магістерської роботи: методи та засоби захисту інформації, стеми управління інцидентами інформаційної безпеки, DLP-системи

Перелік питань, що підлягають дослідженню:

1. Аналіз існуючих DLP-систем
2. Розгортання та налаштування системи попередження витоку інформації
3. Тестування системи управління інцидентами інформаційної безпеки на основі DLP

Перелік графічного матеріалу (за потреби) схеми побудови архітектури DLP-систем, схема алгоритму захисту від несанкціонованого доступу до інформації

Дата видачі завдання "____ " _____ 20____ р.

Керівник магістерської кваліфікаційної роботи _____ Касаткін Д.Ю.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Ляшук В.С.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи	15.11.2023	Виконано
2	Аналіз предметної області	13.04.2024	Виконано
3	Проектування системи	20.05.2024	Виконано
4	Реалізація системи	27.06.2024	Виконано
5	Тестування розробленої системи	11.09.2024	Виконано
6	Оформлення пояснювальної записки	18.10.2024	Виконано
7	Оформлення графічного матеріалу	26.10.2024	Виконано
8	Постерний передзахист	07.11.2024	Виконано

Студент _____ / Ляшук В.С. /
підпис ПІБ

Керівник проекту (роботи) _____ / Касаткін Д.Ю. /
підпис ПІБ

РЕФЕРАТ

Пояснювальна записка: 85 сторінок, 50 рисунків, 4 таблиці, 26 джерел.

ДИСТАНЦІЙНЕ КЕРУВАННЯ ЕЛЕКТРОПРИЛАДАМИ , МОБІЛЬНИЙ ДОДАТОК, ТЕХНОЛОГІЇ КЕРУВАННЯ ЕЛЕКТРОПРИЛАДАМИ, АЛГОРИТМ РОБОТИ ДОДАТКУ, ДІАГРАМИ ПРОЕКТУВАННЯ ДОДАТКУ.

Об’єкт дослідження дипломної роботи – технології управління інформаційною безпекою.

Предмет дослідження дипломної роботи – інструменти захисту інформації та DLP-системи для розслідування інцидентів.

Мета дипломної роботи – реалізація управління інцидентами інформаційної безпеки на базі DLP-систем для запобігання витоку конфіденційної інформації.

Методи дослідження – опрацювання необхідного літературно довідкового матеріалу, методи проектування, розробки та тестування програмного продукту для запобігання витоку даних з інформаційної системи, огляд сучасних технологій та методів управління інформаційною безпекою для реалізації технології управління інцидентами, проведення експерименту.

Проведено аналіз актуальності впровадження систем контролю витоку інформації; аналіз етапів проведення розслідувань інцидентів; проаналізовано процеси управління кібернетичною безпекою; сформовано рекомендації щодо підвищення стійкості DLP систем; реалізовано управління інцидентами інформаційної безпеки, проведено тестування системи інформаційної безпеки з високим рівнем захисту даних.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

DLES (DeviceLock Enterprise Server): Серверна система управління політиками захисту пристроїв у корпоративних мережах.

DLP (Data Loss Prevention): Система запобігання втраті даних, яка допомагає захистити конфіденційну інформацію від витоків.

UBA (User Behavior Analytics): Аналітика поведінки користувачів, яка використовується для виявлення аномальної та потенційно шкідливої активності.

ACL (Access Control List): Список контролю доступу, який визначає права доступу до ресурсів системи.

ЗЗІ (Засоби Захисту Інформації): Засоби, що забезпечують захист інформації від несанкціонованого доступу, зміни або знищення.

ІБ (Інформаційна Безпека): Сукупність заходів та засобів, що забезпечують захист інформаційних ресурсів.

ОС (Операційна Система): Програмне забезпечення, яке керує апаратними ресурсами комп'ютера і забезпечує взаємодію між програмами та апаратурою.

ОЗП (Оперативний Запам’ятовуючий Пристрій): Пристрій, який використовує пам'ять для тимчасового зберігання даних, що активно використовуються.

ПЗП (Постійний Запам’ятовуючий Пристрій): Пристрій, який зберігає дані постійно, навіть після вимкнення живлення.

ПЗ (Програмне Забезпечення): Набір програм, що виконують завдання на комп'ютері.

ВСТУП

Незважаючи на надійність сучасних засобів захисту інформації (ЗЗІ), вони не здатні знизити ризик порушення режиму інформаційної безпеки (ІБ) до нуля, тому виключити появу інцидентів неможливо. Тому, необхідно направити необхідні ресурси на забезпечення проведення службових розслідувань з метою підвищення ймовірності визначити порушника.

Інциденти ІБ – досить поширене явище, що потребує уваги з боку керівництва організації. При цьому ЗЗІ головним чином орієнтовані на запобігання інцидентам ІБ, характеризуються суттєво обмеженими можливостями для проведення службових розслідувань [1].

Інциденти ІБ - це поява однієї чи кількох небажаних чи несподіваних подій ІБ, з якими пов'язана значна ймовірність компрометації штатних операцій та створення загрози інформації [2].

Відмова в обслуговуванні є великою категорією інцидентів ІБ, що мають одну спільну межу. Подібні інциденти ІБ призводять до нездатності систем, сервісів або мереж продовжувати функціонування з попередньою продуктивністю, найчастіше при повній відмові у доступі авторизованим користувачам. Існує два основних типи інцидентів ІБ, що пов'язані з відмовою в обслуговуванні, які створюються технічними засобами: знищення ресурсів та виснаження ресурсів.

Загалом інциденти ІБ «збір інформації» мають на увазі дії, пов'язані з визначенням потенційних цілей атаки та отриманням уявлення про сервіси, що працюють на ідентифікованих цілях атаки. Подібні інциденти ІХ передбачають проведення розвідки з метою визначення наявності мети, отримання уявлення про навколишню її мережеву топологію і про те, з ким зазвичай ця ціль пов'язана обміном інформації або потенційних вразливостей

мети або безпосередньо навколишнього мережного середовища, які можна використовувати для атаки.

Несанкціонований доступ – це доступ до інформації, що порушує правила розмежування доступу використанням штатних засобів, що надаються засобами обчислювальної техніки чи автоматизованими системами [1].

При проведенні службових розслідувань ефективним засобом формування доказової бази виступає система запобігання витоку даних. Оскільки DLP-система мають потужні засоби аудиту, механізми тіньового копіювання та контекстного аналізу даних, що передаються за межі організації чи робочих станцій. Контекстний аналіз представляє собою перевірку вмісту документів на предмет наявності конфіденційної інформації, а тіньове копіювання – приховане збереження на сервері переданих та файлів, що відриваються. Тому застосування технології управління інцидентами інформаційної безпеки з використанням DLP-систем є актуальною задачею.

1. Аналіз предметної області та визначення актуальності

1.1. Основні поняття у сфері систем попередження витоку даних

Розслідування інцидентів є важливим завданням для систем Data Loss Prevention (DLP). Це програмні рішення, які розроблені для запобігання витоку даних. Компанії, які не хочуть зазнати репутаційних, фінансових або інших втрат, використовують такі ситеми для захисту корпоративної інформації. Але DLP не обмежуються лише витоками. Системи почали зростати вглиб, покращуючи якість аналізу та перехоплення контенту. Вони швидко стали потрібні в HR-відділах, у економістів, управлінців, спеціалістів з інформаційної безпеки (ІБ) [3].

Система DLP, зазвичай, це модульний програмний продукт, рідше апаратний продукт. Вона базується на аналізі потоків даних, що виходять за межі мережі та/або її певного сегмента. На рисунку 1.1 наведена схема мережі компанії, яка турбується про безпеку інформації та впровадила DLP в корпоративну мережу.

Сучасна система DLP складається з трьох базових модулів із можливістю інтеграції новітніх технологій [4]:

- Аналізатор – це мережевий компонент, що контролює трафік, збирає статистику про мережеві потоки та взаємодіє із засобами глибокого аналізу DPI (Deep Packet Inspection) для виявлення аномалій у реальному часі. Деякі системи інтегрують алгоритми машинного навчання для аналізу поведінки користувачів і виявлення потенційних ризиків.
- Система зберігання даних – включає розподілену архітектуру для зберігання та обробки великих обсягів інформації, підтримуючи шифрування і сегментацію даних для підвищення безпеки.

- Графічний модуль – не лише візуалізує дані, але й надає розширені інструменти аналітики, включаючи дашборди з можливістю інтеграції з SIEM (системами управління інформацією та подіями безпеки). Такий модуль допомагає працівникам інформаційної безпеки приймати обґрунтовані рішення на основі зібраних даних.

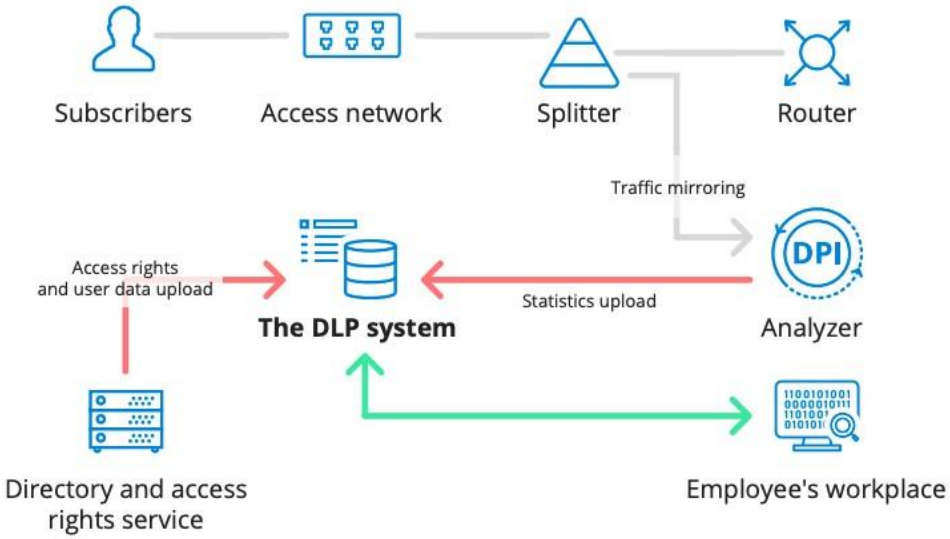

Рисунок 1.1 - Схема мережі компанії з DLP системою

В деяких DLP системах є зовнішній модуль, що призначений для безпосереднього встановлення на ПК користувача для подальшого моніторингу натискань клавіш на клавіатурі, зображення на екрані монітора, вмісту оперативної пам’яті, а також контролю переміщення/ копіювання / видалення файлів на дискових пристроях.

Такий склад системи можна вважати ідеальним, якщо її доповнити Deep Packet Inspection (DPI) – технологією глибокого аналізу трафіку [2]. Завдяки DPI система DLP може:

- проводити аудит безпеки мережі та виявляти зовнішні атаки, а також вживати контрзаходів для їх усунення за допомогою оповіщення персоналу;
- аналізувати стан всіх мережевих з'єднань і прийняти рішення про їх розрив;

- здійснювати збір статистику протоколів, додатків, сервісів, а також напрямок трафіку і навіть для конкретного користувача з подальшим логуванням;
- генерувати трафік для цільового сервера, щоб перевірити його продуктивність і стійкість до атак.

Особливістю DLP є те, що це не система для стеження за співробітниками, а скоріше фільтр, який не дає втекти назовні чутливим даним DLP - це рішення для запобігання витоку конфіденційних файлів за межі мережі компанії. Такі системи аналізують всю вхідну та вихідну інформацію та за допомогою неї виявляють підозрілі операції та ризики.

DLP-рішення закривають кілька проблем захисту інформації, зокрема [5]:

- аналізують та маркують дані, що відносяться до конфіденційних;
- сканують потоки даних кожного співробітника компанії у кожному каналі зв'язку, виявляючи інформацію, що не підлягає розголошенню;
- спотворюють або видаляють відомості, що залишають межі робочої мережі.

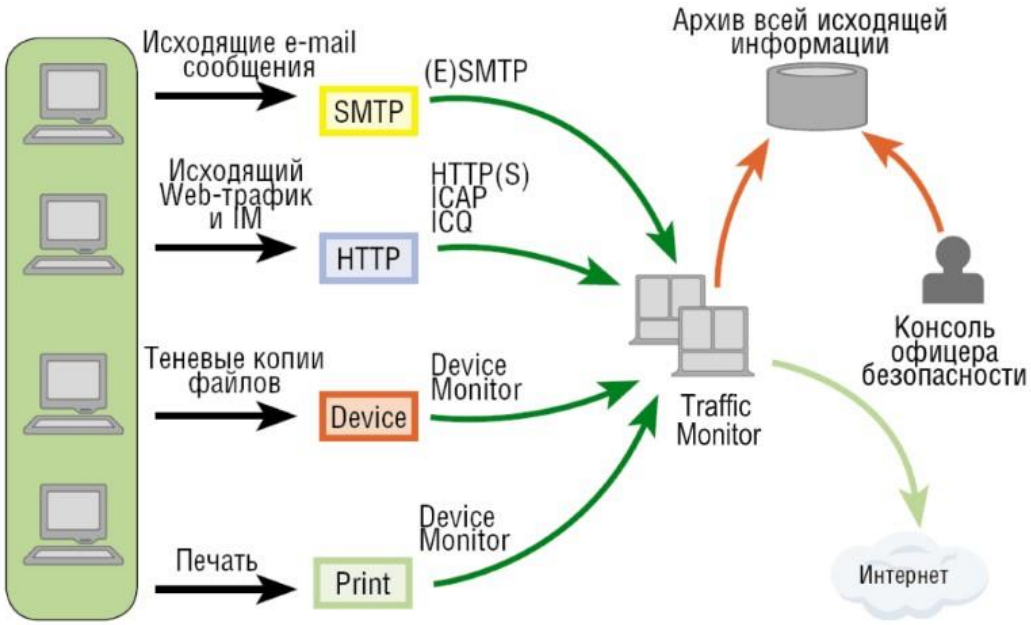

Рисунок 1.2 - DLP-рішення налізу даних

DLP-системи працюють наступним чином. Всі рішення відрізняються один від одного, хоч і переслідують одну мету. Компанії створюють продукт, ґрунтуючись на своєму розумінні безпеки та своєму досвіді, впроваджують здавалося їм вдалими рішеннями, тим чи іншим способом закривають «вузькі» місця. DLP-рішення можна розділити за принципом роботи і можна виділити наступні [6]:

- системи з активним контролем дій користувача;
- системи пасивним контролем дій користувача;
- гібридна модель системи.

Рішення з активним контролем – це системи, які сканують усі види трафіку, виявляючи ризик витоку у 99% випадків. Вони постійно працюють, «їдя» багато ресурсів. І при цьому здатні зупинити весь бізнес або бізнеспроцес до з'ясування деталей інциденту. Користуватися таким інструментом треба акуратно, оскільки він складний та чутливий. Як правило, це доручають відділу інформаційної безпеки.

Рішення з пасивним контролем - це програмовані фільтри, що працюють із певними типами загроз (типовими). Вони проводять постійний аналіз критичних каналів передачі даних, їм не потрібна допомога людини, крім при налаштуванні на самому початку роботи. Такі системи ефективні при грубих спробах несанкціонованого доступу та випадкових витоків. Оскільки система здатна працювати у фоновому режимі сама, її використовують у багатьох компаніях. Але від цілеспрямованої атаки таке рішення не рятує.

Гібридна модель - такі рішення більшість завдань (включаючи моніторинг трафіку) відводять пасивної системі контролю, а роботу з активним функціоналом і відображенням нових загроз доручають відділу інформаційної безпеки.

У багатьох компаніях необхідний рівень безпеки досягається рахунок використання корпоративної електроніки. Ноутбук, телефон, планшет із

зашитою DLP-системою контролюють та обмежують можливості обміну конфіденційною інформацією. Якщо такий варіант здається дорогим, є спосіб здешевити його. Достатньо дозволити персоналу використовувати особисті гаджети, але з корпоративним DLP.

Крім сканування трафіку, DLP-рішення виконують розмітку перехоплених даних. Архів перехоплення - це просто невпорядкована купа даних, працювати з якою майже неможливо. Навіть повнотекстовий пошук не виправить ситуацію. Наприклад: у компанії прийнято 12-символьні номери договорів. Їх можна вказувати з відбивкою через кожні 4 символи, разом, з символом # / № або без них. Знайти вручну «зливаються» договори важко. А комп'ютерна система з цим впорається швидко та ефективно. На екрані буде видно скільки разів, коли, ким пересилалися ці відомості. Розмітка даних допоможе ІБ розібратися, на що потрібно звернути особливу увагу під час захисту даних. І, можливо, спонукає змінити права доступу для відділів чи конкретних посад.

Моніторинг активності, який ведеться завдяки впровадженню DLP, дозволяє контролювати як офісних співробітників, так і віддалених. Безумовно, це не єдина міра ефективності персоналу, але якщо людина активна 4 години з 8 необхідних — це вже потребує розгляду.

Аналіз ланцюжків подій – ще одна важлива функція DLP. Продукти класу UBA (User Behavior Analytics) аналізують поведінку користувача у його робочому інформаційному середовищі [7]. Завдяки хорошій розмітці подій, система може показати, чим насправді займається співробітник: працює, відвідує «заборонені» сайти, просто сидить в інтернеті або відправляє резюме, дивиться вакансії. Тобто система вибудовує події в ланцюжок, допомагаючи зрозуміти, чи ефективний співробітник, чи ризики співпраці з ним, чи планує він звільнення. Так само можна виявити афілірування з компанією-підрядником тощо. буд. Комп'ютерний аналіз життєвих ситуацій дозволяє прогнозувати ризики, знаходити збої та вузькі місця у бізнесі.

Пропозиції на ринку вказують на наявність загальних ключових характеристик, що дозволяють віднести рішення ІБ до класу DLP-систем, зокрема:

- тотальний контроль каналів витоку;
- аналіз інформації;
- блокування витоків;
- архівування інформації.

Основні канали витоку інформації складають дві великі групи:

- локальні (USB, принтери, а також будь-які периферійні пристрої, на які можна скопіювати конфіденційну інформацію);
- мережеві канали (такі як електронна пошта, інтернет-месенджери, соціальні мережі, сайти, форуми, блоги та ін.);

DLP-системи перехоплюють весь трафік, що виходить за межі корпоративної мережі підприємств, та аналізують його на наявність конфіденційної інформації [8]. У передових DLP-системах виявлення конфіденційних даних зазвичай використовуються такі технології як цифрові відбитки, лінгвістичний аналіз, аналіз графічних файлів (OCR), самонавчальні технології, та інших.

На підставі даних аналізу вмісту DLP-система приймає рішення відповідно до встановлених політик безпеки про дозвіл або заборону передачі повідомлення, запису або друку файлу.

Весь трафік, що перехоплюється DLP-система поміщає у свій архів, що створює повноцінну базу для розслідування інцидентів інформаційної безпеки.

Існують різні підходи до класифікації DLP-систем. Класифікація важлива для порівняння DLP приблизно одного рівня та вибору для впровадження найкращого рішення. DLP-систем поділяються на декілька типів, в залежності від різних (рисунок 1.3).

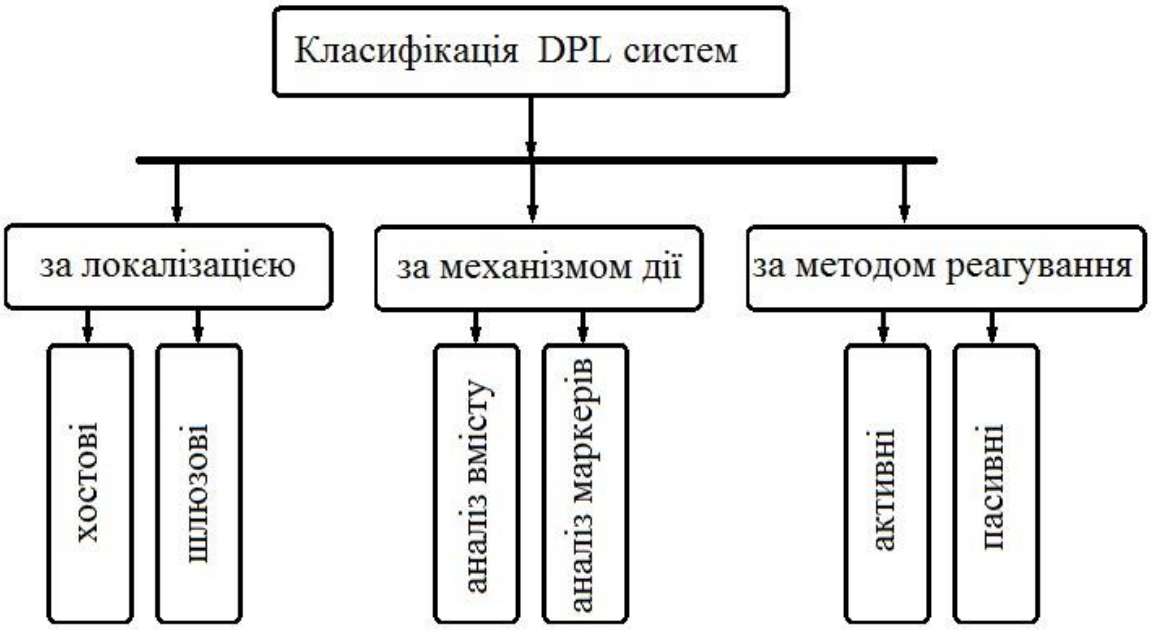

Рисунок 1.3 – Класифікація DLP-систем

За локалізацією (мережевою архітектурою) DLP-системи поділяються [9]:

- хостові - засновані на роботі агента, що безпосередньо інстальовані на локальному комп'ютері кінцевого користувача, що зручно коли необхідно проконтролювати його відокремлені дії (запис інформації на носій, введення сумнівних пошукових запитів);
- шлюзові - розташовуються на проміжних шлюзах та перевіряють мережевий трафік.

Хостові DLP-системи дозволяють контролювати діяльність користувачів ПК, реєструють всі дії та передають їх в централізоване сховище, що дозволяє співробітникам відділу ІБ отримати повну картину того, що відбувається. Використання програм-агентів обмежує сферу застосування таких систем, вони можуть бачити лише локальні або мережеві пристрої, які підключені безпосередньо до тих ПК на яких вони працюють. Функціональна схема DLP-системи хостового рішення наведена на рисунку 1.4.

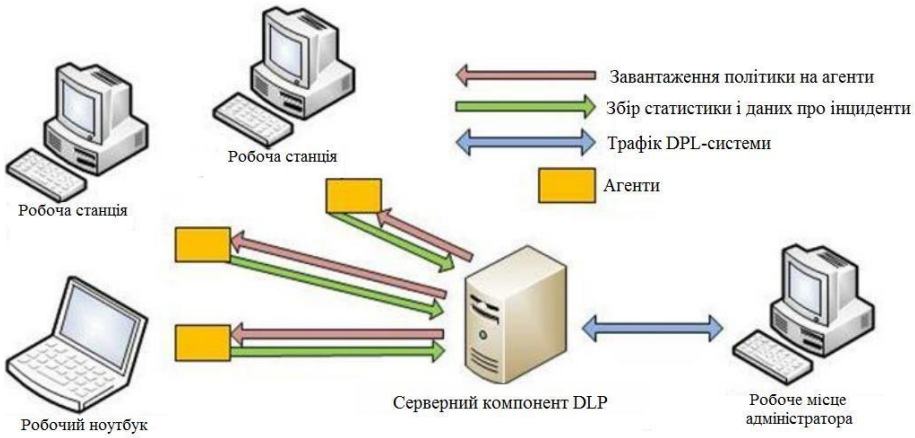

Рисунок 1.4 - Функціональна схема хостової DLP-системи

Перевагами таких систем є широкі можливості для контролю і блокуванню дій користувачів, наприклад, для протидії випадкам нецільового використання ПК. До недоліків слід віднести складний процес впровадження в експлуатацію та подальше адміністрування. При будь-якій зміні правил безпеки адміністратору необхідно забезпечити їх поширення на всі кінцеві станції мережі. Також невелика захищеність системи від несанкціонованого втручання в її роботу зі сторони користувачів є вагомим недоліком.

Шлюзові системи забезпечують захист від витоків інформації через протоколи мережі традиційних інтернет-сервісів: HTTP, FTP, POP3, SMTP та ін. Контролювати те, що відбувається на кінцевих точках корпоративної мережі з їх допомогою неможливо На рисунку 1.5 наведена функціональна схема шлюзового рішення DLP-системи в режимі блокування, а на рисунку 1.6 в режимі моніторингу.

Перевагами є швидкість введення в експлуатацію, зручність обслуговування та керування. Також високий ступінь захисту від несанкціонованого втручання в її роботу зі сторони користувачів. Недоліками – обмежена область застосування та проблематичність контролю деяких видів мережевого трафіку.

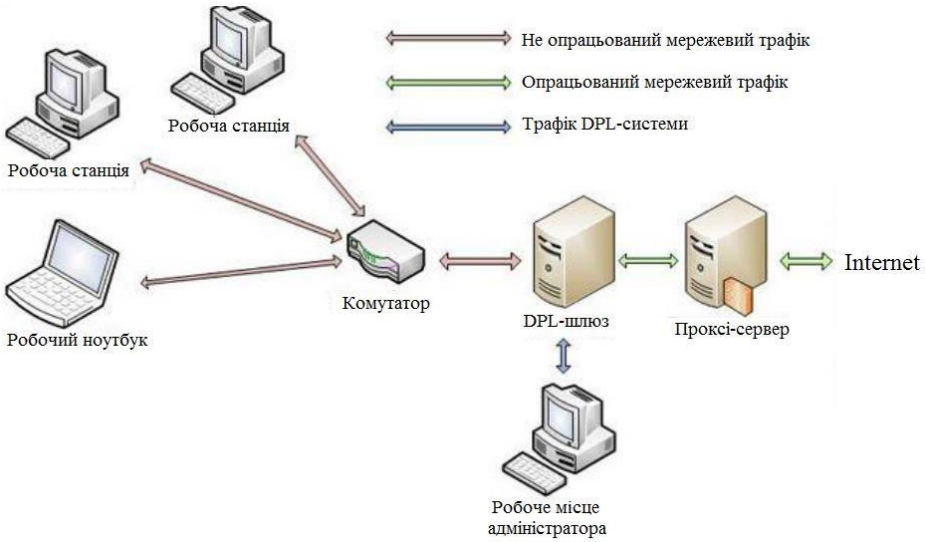

Рисунок 1.5 – Функціональна схема шлюзового рішення DLP-системи в режимі блокування

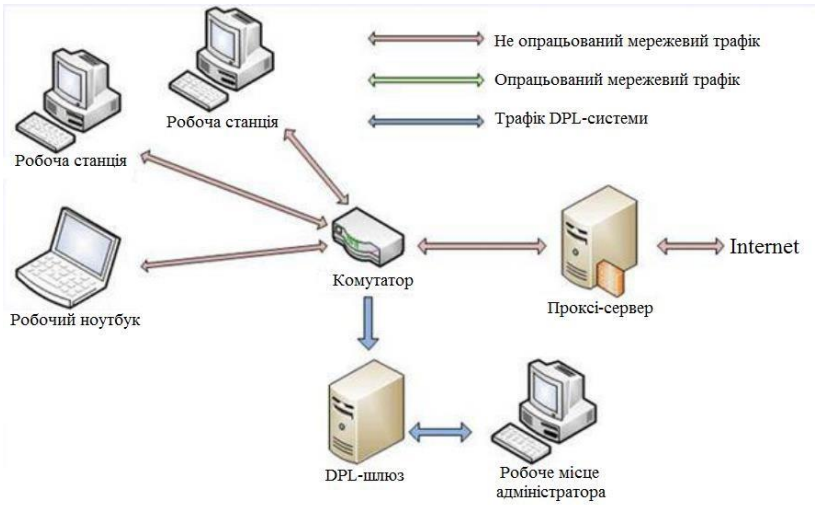

Рисунок 1.6 – Функціональна схема шлюзового рішення DLP-системи в режимі моніторингу

Сучасні розвинені системи із запобігання витоків даних зазвичай поєднують у собі і хостовий, і шлюзовий компонент. При цьому, в ідеалі, розбираються всі вихідні потоки інформації [10]:

- передача даних через інтернет;
- запис документів на зовнішній носій;
- відправка їх на друк;
- пересилання через Bluetooth та інші дії користувача.

За механізмом визначення ступеня конфіденційності даних, що передаються, виділяють два види DLP-систем:

- системи, що встановлюють конфіденційність на основі аналізу маркерів документа;
- системи, які проводять аналіз вмісту документа.

Під першим способом розуміється перевірка назви, заголовків, підписів та грифів документа. Цей варіант швидший, але нестійкий перед ситуацією, як у маркери документа вносяться зміни. Другий спосіб вимагає великих ресурсів, але він надійніший з позиції можливого видалення грифів перед відправкою файлу або зміни його назви на незначне з точки зору моніторингу. До того ж, він піддається кращій масштабованості, оскільки кількість документів, що обробляються системою, не залежатиме від їх спеціальних міток.

Ще один поділ DLP-систем базується на методах їх реагування на загрози, що виникли, зокрема виділяють [11]:

- активні системи, які негайно переривають сумнівний процес, тим самим попереджаючи можливу шкоду,
- пасивні системи, які лише фіксують підозрілі факти, оформляючи їх у звіти для подальшого аналізу з боку служби безпеки.

Активні DLP-системи є кращими, якщо основним завданням є запобігання інцидентам, але вони здатні несподівано зупинити бізнес-процеси компанії в невідповідний час. Пасивні DLP-системи покликані боротися із систематичними порушеннями та реагувати на них за фактом. Не впливаючи безпосередньо протягом бізнес-процесів організації, вони передбачають аналітичну роботу над логами з боку підготовлених фахівців.

Також DLP-системи поділяються на три типи:

- системні - на рівні хоста;
- мережеві - на рівні мережі;

- прикладні - як правило, рівня СУБД).[12].

Також DLP-системи можна класифікувати за їх розміщенням [8]:

- у мережах - Network DLP;
- у кінцевих пунктах призначення даних (Endpoint DLP).

Крім того, засоби DLP можна класифікувати за можливими станами даних, на роботу з якими вони орієнтовані [7]:

- дані у стані спокою (data at rest);
- у процесі переміщення (data in motion);
- в процесі використання (data in use).

Кожному з таких станів адресується свій власний набір технологій, наприклад підходи, що лежать в основі Network DLP, простіше, більш традиційні та дешевші, але менш ефективні[9].

На ринку є багато компаній, що готові запропонувати подібний продукт, наприклад:

- Spectre;
- McAffee;
- Searchinform;
- DeviceLock DLP;
- Dell EMC RSA DLP;
- Zecurion DLP;
- Symantec DLP.

Продукти цих компаній дозволяють вирішити проблему захисту від витоку даних, але не кожна з них може зробити це максимально ефективно, використовуючи технологію DPI для обробки всього трафіку в корпоративній мережі. Використання технології глибокого аналізу трафіку дозволяє проводити перевірку на рівні протоколу та програми, аналізувати до рівня OSI 7, який недоступний для інших систем DLP.

Суть роботи систем полягає в тому, що потрібно проводити аналіз усієї інформації, яка виходить або входить, а також циркулює всередині підприємства. Дана система з використанням алгоритмів аналізує дані і не дає критичної інформації проникнути, куди їй не належить. Тобто здійснюється блокування передачі даних та інформує про підозрілу діяльність.

В основі DLP системи лежить набір правил, які можуть відрізнятися своєю складністю та торкатися конкретних аспектів роботи. І за порушення відповідальний співробітник отримує відповідне повідомлення.

Наприклад, у певній компанії виявили працівника, який займався майнінгом, з метою отримання криптовалюти та особистої вигоди. У цьому допоміг спеціальний модуль активності користувачів, і звіт говорить про те, що робоча станція вночі не відключалася. Вочевидь, у разі слід запустити аналіз запущених процесів, і тут буде видно, які процедури виконував той чи інший співробітник.

Система стежить як за часом роботи, а й виявляється активність використовуваних програм на ПК. В цілому, це стосується практично будь-якої інформації, які дані вводилися з клавіатури, листування, передача даних електронною поштою, обмін файлами в соціальних мережах і різного роду месенджерах. Перелік завдань, які відстежує система, обширний, це навіть включає список документів, відправлених на друк, SIP-телефонію і навіть активність на сторонніх сайтах.

Для аналізу даних система насамперед має їх отримати. Це може бути виконано наступними способами перехоплення даних серверний та агентський.

Перший варіант передбачає контроль системою мережевого трафіку безпосередньо на сервері. В іншій ситуації стороннє, агентське програмне забезпечення (ПЗ) встановлюється на кожен окремий комп'ютер співробітника, і дана програма відповідальна за аналіз інформації.

Останній варіант на даний момент вважається найбільш поширеним, так як завдяки агентам можна отримати найрізноманітніші дані з використанням різних каналів комунікації, тобто це чудова можливість запобігти будь-яким витокам.

1.2. Аналіз актуальності використання систем контролю витоку інформації

Будь-яка компанія, яка зацікавлена у збереженні комерційної таємниці та інших важливих відомостей, утриманні цінних кадрів, виявленні відвертих «шкідників», вживає заходи щодо захисту даних. Пасивні DLP-системи доступні більшості компаній, гібридні більше підходять організаціям, які виросли з категорії малого бізнесу, але ще не стали великим. Активні вибирають великі компанії, які готові платити за гідний рівень захисту.

Важливо розуміти, що ефективність DLP визначається її непомітністю. Керівник не дихає в потилицю своїм співробітникам, не ставить дві камери на кожне робоче місце. Але при цьому знає, як працює кожна людина, хто ефективний, а хто слабка ланка. Комфортно обом сторонам, і в цьому сила комп'ютерних систем контролю [11].

DLP-рішення потрібні перш за все для корпоративної інформації, адже це не лише клієнтська база. Це розробки, відомості про продаж, плани розвитку, інші цінні відомості. Якщо ця інформація опиниться поза компанією, наслідки можуть бути сумними. Щоб контролювати потоки інформації, але не заважати співробітникам користуватися внутрішніми базами даних, використовують комп'ютерні системи захисту даного класу.

DLP-система дозволяє контролювати канали передачі даних, виявляти та запобігати витоку критичної інформації. Вона гнучко класифікує дані всередині компанії, контролює їхні потоки. Також з її допомогою зручно шукати дані у файлових сховищах, робочих комп'ютерах співробітників, базах даних тощо.

Досить часто співробітники викликають витік не спеціально - причинами є неуважність, недбалість або некомпетентність. Однак випадки викрадення файлів з метою подальшого продажу конкурентам, помсти або відкриття власної компанії на основі унікальної інформації є також досить поширеними.

Звичайно, гарантувати абсолютний захист від наслідків діяльності працівників не може жодна DLP-система, проте вона дозволяє значно мінімізувати ризики та наслідки людських помилок, а також забезпечують дотримання положень щодо захисту конфіденційних даних.

Потреба в DLP-системах постійно зростає через збільшення кількості витоків даних у різних галузях. Наприклад, у 2023 році витік конфіденційних даних із хмарного сховища одного з найбільших технологічних гігантів призвів до розголошення інформації про мільйони користувачів, що спричинило значні фінансові втрати та пошкодження репутації компанії. Також у тому ж році була зафіксована масштабна атака на фінансовий сектор, де хакери використали соціальну інженерію для обходу стандартних систем захисту.

З розвитком дистанційної роботи та використанням хмарних середовищ важливість DLP-систем значно зросла. Вони дозволяють контролювати потоки даних у корпоративних і хмарних мережах, забезпечуючи виявлення і запобігання витокам незалежно від місцезнаходження співробітників. DLP-системи також допомагають компаніям дотримуватися вимог законодавства, таких як GDPR, CCPA та інші, що є критичним для уникнення штрафів і підтримки репутації.

У сфері IT-технологій швидко набирає популярності сегмент DLP-систем: ринок таких рішень нарощує обороти, а самі системи швидко вдосконалюються та переходять мовні бар'єри. Це пов'язано з тим, що з боку політики управління підприємствами все більша увага приділяється запобіганню витоку інформації конфіденційного характеру. Втрата

внутрішніх напрацювань, перехід перспективних бізнес-ідей до конкурентів, попадання фінансової інформації до третіх рук - ось лише мала частина причин, чому важлива інформаційна безпека організації. Все це може обернутися настільки значними фінансовими та репутаційними втратами, що витрати на використання DLP-системи в порівнянні виявляться несуттєвими. Потреба захисту корпоративних даних пов'язана і з розвитком віддаленої роботи, коли комп'ютер, позиціонований як службовий (як мінімум частину часу протягом доби), фізично може перебувати поза периметром підприємства, що не знімає важливості коректного поводження з довіреною інформацією.

Однак інформаційна безпека підприємства– це головне, але далеко не єдине завдання DLP-систем [2]. Крім того, що вони створюють захищений цифровий контур, куди не проникають зовнішні загрози, а внутрішні важливі дані не переходять його меж, такі програмні продукти використовуються для моніторингу роботи персоналу, оцінки його продуктивності та відповідності посади. Таким чином, сучасні DLP-системи – це універсальні засоби для всеосяжного контролю безпечної та ефективної роботи компанії.

Майже всі великі компанії приділяють належну увагу зовнішнім загрозам, і це стосується не тільки спаму, а й фішинг-атак, вірусів, підміни сторінок різних інтернет-порталів, навіть реклами та шпигунських програм [6]. Але варто зазначити, що не треба забувати про внутрішні загрози, які можуть завдати значно більшої шкоди порівняно з весняними загрозами.

Адже, будь-який співробітник компанії може виступати як потенційний інсайдер і тим самим може поставити під загрозу інформаційну безпеку підприємства. Це може бути не злий намір, а банальна необережність чи помилка, від цього ніхто не застрахований ні рядовий співробітник, ні менеджер, ні керівництво. Тобто використання DLP системи стане вірним рішенням і допоможе уникнути проблем.

На рисунку 1.7 наведено фінкції DLP-систем. Основними функціями DLP-систем є наступні:

- контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skype, ICQ та інших програм та протоколів;
- контроль збереження інформації на зовнішні носії - CD, DVD, flash, мобільні телефони тощо;
- захист інформації від витоку шляхом контролю виведення даних на друк;
- блокування спроб пересилання/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання карантинної папки;
- пошук конфіденційної інформації на робочих станціях та файлових серверах за ключовими словами, мітками документів, атрибутами файлів та цифровими відбитками;
- запобігання витоку інформації шляхом контролю життєвого циклу та руху конфіденційних відомостей.

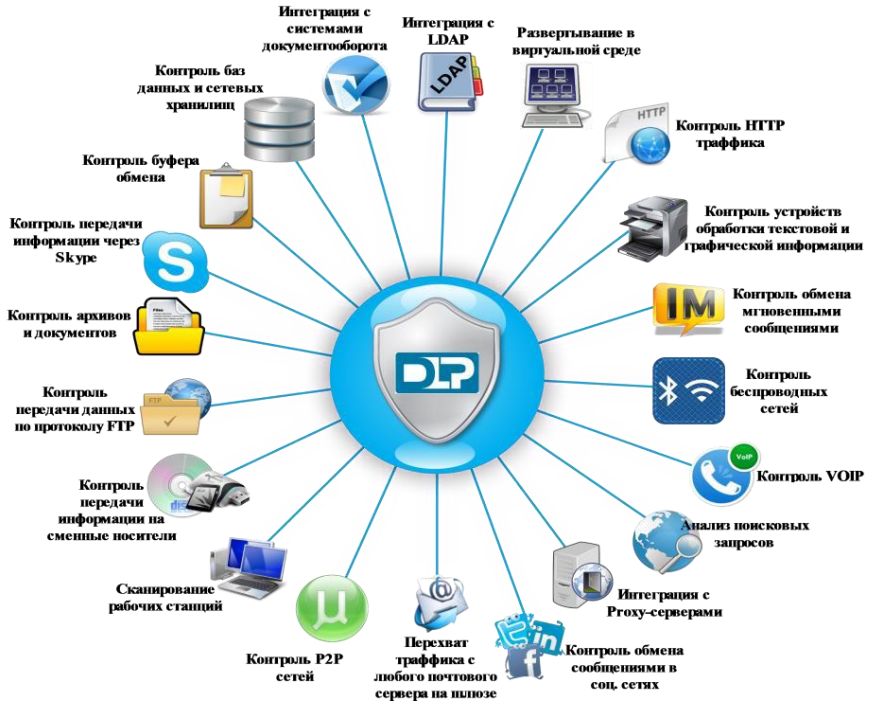

Рисунок 1.7 – Функції DLP-систем

Використання даної системи дозволяє стежити за передачею даних і запобігати витоку, але за рахунок певних особливостей додатково реалізує такі функції:

- аналіз завантаженості працівників - численні системи можуть облік зайнятості персоналу, і DLP перестав бути винятком;
- юридичну підтримку - якщо справа доходить до судових розглядів, то дані можуть бути доказами неправомірних дій;
- додаткову мотивацію - коли працівник знає, що його діяльність контролюється, то підвищується відповідальність та покращується ефективність.
- сховище даних - система зберігає інформацію, і містить усі дані кожного співробітника.

За допомогою DPL-систем вирішуються наступні задачі:

- запобігання витоку конфіденційної інформації за основними каналами передачі даних:
  - вихідний інтернет-трафік (HTTP, FTP, P2P та ін.);
  - вихідна та внутрішня електронна пошта;
  - системи миттєвого обміну повідомленнями;
  - мережевий та локальний друк;
- контроль доступу до пристроїв і портів вводу-виводу, до яких належать:
  - дисководи,
  - USB - пристрої,
  - Інфрачервоні потри,
  - LPT потри;(принтери);
  - COM порти (модеми).

Захист конфіденційної інформації в DLP-системах може здійснюватися за трьома рівнями:

1 рівень - Data-in-Motion - дані, що передаються мережевими каналами:

- web (HTTP/HTTPS протоколи);
- служби миттєвого обміну повідомленнями;
- корпоративна та особиста пошта (POP, SMTP, IMAP тощо);
- бездротові системи (WiFi, Bluetooth, 3G тощо);
- ftp – з'єднання.

2 рівень - Data-at-Rest - дані, що статично зберігаються на:

- сервери;
- робочих станціях;
- ноутбуки;
- системах зберігання даних (СЗД).

3 рівень – Data-in-Use – дані, що використовуються на робочих станціях, де система класу DLP включає такі компоненти:

- центр управління та моніторингу;
- агенти на робочих станціях користувачів;
- мережевий шлюз DLP, що встановлюється на Інтернет-периметр.

У системах DLP конфіденційна інформація визначається за допомогою ряду різних ознак, а також у різні способи, основними з яких є:

- морфологічний аналіз інформації;
- статистичний аналіз інформації;
- регулярні вирази (шаблони);
- метод цифрових відбитків;
- метод цифрових міток.

Використання DLP-систем давно стало вже не просто модою, а необхідністю, адже витік конфіденційних даних може призвести до величезних збитків для компанії, а головне зробити не одномоментний, а тривалий вплив на бізнес компанії. У цьому шкода може мати як прямий, а й

непрямий характер. Тому що, крім основного збитку, особливо у разі розголошення відомостей про інцидент, Ваша компанія «втрачає обличчя». Збитки від втрати репутації оцінити в грошах дуже складно! Адже кінцевою метою створення системи забезпечення безпеки інформаційних технологій є запобігання або мінімізація шкоди (прямої чи непрямої, матеріальної, моральної чи іншої), що завдається суб'єктам інформаційних відносин за допомогою небажаного впливу на інформацію, її носії та процеси обробки.

Якщо система для захисту персональної інформації дійсно потрібна, виникає питання, яким чином вибрати відповідний варіант, адже сьогодні є велика різноманітність система на ринку. Насамперед потрібно визначити кілька ключових питань:

- канали передачі даних, які має контролювати система;
- ПЗ використовуватиметься виключно для перехоплення, або також потрібно здійснювати контроль;
- бюджет для придбання системи;
- обладнання для роботи, що використовується.

Щоб зрозуміти, який варіант найкраще підійде, потрібно обрати декілька програм і запросити демонстраційну версію. Тобто наочна демонстрація допоможе вирішити всі проблеми та відповість на всі запитання. Саме тестовий період покаже, наскільки якісний продукт і чи він відповідає поставленим завданням.

Налаштована DLP-система повинна запобігати будь-якому витоку конфіденційної інформації за межі корпоративного периметра.

Переваги використання DLP-систем полягають в наступному:

- захищати інформаційні активи організації від неправомірних дій, передачі третім особам та несанкціонованого доступу;
- мінімізувати ризики втрати критично важливої для бізнесу інформації;

- зменшити ризик втрати стратегічно важливої інсайдерської інформації;
- досягти економії коштів: використання системи захисту від витоків допоможе скоротити інші витрати, пов'язані з управлінням даними та безпекою;
- зменшити витрати на дотримання вимог законодавства у сфері захисту персональних даних.

Основні переваги систем DLP, на відміну від альтернативного рішення, такими як продукти шифрування, розмежування доступу, контролю доступу до змінних носіїв, архівування електронної кореспонденції, статистичними аналізаторами, полягають в забезпеченні:

- контролю над усіма каналами передачі конфіденційної інформації в електронному вигляді (включаючи локальні та мережеві способи), що регулярно використовуються у повсякденній діяльності;
- виявленні інформації, що захищається за її вмістом (незалежно від формату зберігання, каналів передачі, грифів та мови);
- блокуванні витоків (припинення надсилання електронних повідомлень або запису на USB-накопичувачі, якщо ці дії суперечать прийнятій в компанії політиці безпеки);
- автоматизації обробки потоків інформації відповідно до встановлених політик безпеки (впровадження DLP-системи не вимагає розширення штату служби безпеки).

Основне призначення DLP – забезпечувати захист від випадкового чи навмисного поширення конфіденційної інформації з боку працівників, які мають доступ до інформації через свої посадові обов'язки. Але, крім того, будьяка DLP може бути налаштована і для боротьби зі зловмисними інсайдерами.

Тим не менш, DLP не можуть у прямому сенсі запобігти всім витокам, оскільки існують людський фактор, хакерські способи обходу системи.

Комерційна доцільність даних систем полягає у значному зниженні ризиків витоку інформації з необережності та у частковому зниженні ризиків навмисного крадіжки конфіденційних відомостей [9].

До недоліків DLP систем можна віднести те, що алгоритми фільтрації, не завжди можуть відрізнити конфіденційні дані від публічних, на практиці ефект не завжди досягається.

Ще одне обмеження концепції DLP пов'язане з її архітектурою. Системи даного класу повинні, з одного боку, розбирати різні протоколи, з іншого — отримувати текстовий вміст із файлів різних форматів. Як наслідок, розробникам DLP доводиться вплутуватися в нескінченну гонку з підтримки нових і нових технологій. Часто деякі протоколи та формати підтримуються не повністю, наприклад, без можливості блокування.

Ще одним концептуальним недоліком DLP є труднощі сканування інформації на робочих станціях користувачів. У тих випадках, коли дані залишають корпоративний периметр локальними каналами (USB, CD/DVD, принтери), інформація не потрапляє на рівень мережевого шлюзу. Як наслідок, доводиться або пересилати централізований сервер, або аналізувати локально.

В обох випадках виникають проблеми, пов'язані з ефективністю фільтрації або підвищеним навантаженням на локальні машини та мережеві канали.

Незважаючи на всі перераховані обмеження, працююча DLP-система повинна запобігати будь-якому витоку конфіденційної інформації за межі корпоративного периметра.

1.3. Постановка завдання проектування

Проведений дослідження дозволили визначити поняття DPL-системи, їх будову та сфери застосування. Після аналізу існуючих систем контролю

витоку інформації, визначено їх основні функції та задачі, які вони дозволяють вирішувати. Проведена класифікація DPL-систем дозволила провести порівняння і здійснення вибору для впровадження найкращого рішення. Виявлено переваги та недоліки DPL-систем. Виявлено, що існує велика кількість засобів попередження витоку даних, але універсальної відповіді на питання, яка DLP-система кращі, не існує. Система, яка блокує лише передачу даних через мережу, але не контролює порти комп'ютера або система, що контролює USB-порти, але не стежить за SATA, і будь-хто, хто має фізичний доступ до системної плати комп'ютера, зможе легко підключити свій диск і переписати конфіденційні дані не є повноцінною. Вибір залежить виключно від потреб компанії та від підходу внутрішньої служби ІБ до боротьби з таким видом шахрайства, як витік інформації. Головним критерієм є те, наскільки добре система може детектувати конфіденційну інформацію і який буде відсоток помилкових спрацьовувань.

В результаті, можна сказати, що завданням для проектування є застосування технології управління інцидентами інформаційної безпеки з використанням DPL-систем. В результаті про будь-яку сумнівну дію користувача, здатну спровокувати інцидент ІБ або порушення робочого режиму, відповідальна особа миттєво повідомляється системою за допомогою електронної пошти. Це дозволить оперативно вжити заходів щодо нівелювання загрози.

Також використовуючи детальні протоколи про запуск додатків та інтервали роботи в різних програмах, можна зробити висновок про те, що моніторинг охопить всі основні аспекти діяльності користувача за ПК, як з точки зору продуктивності, так і протидії інцидентам. При цьому аналіз зібраних даних не потребуватиме великих часових затрат або спеціальної підготовки, оскільки відбуватиметься візуалізація звітів, діаграми та графіки, що полегшить прийняття управлінських рішень.

1.4. Висновки до розділу

1) Розглянуто основні поняття систем попередження витоку даних. Повноцінною є система, що дозволяє здійснювати блокування передачі з будьякого інтерфейсу комп'ютера.

2) Проведений аналіз актуальності використання систем контролю витоку інформації. Розвиток цифрових технологій та соціальної інженерії ставить під сумнів безпеку конфіденційної інформації, тому важливо зробити вибір на користь перевіреного рішення – DLP-системи. Оскільки використання DLP дозволять навіть при високій швидкості аналізувати потоки даних, що виходять за межі корпоративної мережі і запобігати витоку конфіденційної інформації за межі корпоративної мережі.

3) Відповідно до вимог сьогодення з метою задоволення попиту на технології управління інформаційної безпеки сформульоване завдання проектування метою якого є реалізація управління інцидентами інформаційної безпеки на базі DLP-систем, що забезпечить мінімізацію ризиків інформаційної безпеки або захист конфіденційної інформації від внутрішніх загроз.

2. Постановка завдання проектування

2.1. Етапи проведення службових розслідувань інцидентів

Можна виділити такі етапи проведення службових розслідувань[13,14]:

- етап організації службового розслідування;
- етап проведення службового розслідування;
- етап прийняття рішення.

На етапі організації службового розслідування ініціатором службового розслідування є директор чи начальник підрозділу. Службове розслідування призначається у випадку виявлення порушення, що здатні завдати:

- шкоду здоров'ю, безпеці та добробуту працівників;
- шкоду безпеці та добробуту організації;
- втрату довіри до організації в клієнтів, партнерів і громадськості;
- фінансові санкції організації та/або працівникам.

У випадку ухвалення рішення про проведення службового розслідування, керівником організації призначається комісія, яка проводить розслідування. Співробітник, щодо якого проводиться розслідування, повинен бути повідомлений про організацію щодо нього службового розслідування у письмовій формі з вказанням причин, через які воно було ініційоване.

Співробітник, щодо якого проводиться розслідування, має право на захисника. Захисник має право бути присутнім на засіданнях комісії з даного службового розслідування, дізнаватися факти, що належать до справи, і рекомендувати своїх свідків. Захисник не має права заважати проведенню дізнання, відповідати на запитання комісії замість працівника, щодо якого проводиться розслідування. Розслідування носить конфіденційний характер, оскільки розголос цієї інформації може призвести до появи небажаних чуток.

На етапі проведення службового розслідування комісія здійснює аналіз наданих матеріалів, включаючи записи відеоспостереження, журнали подій, мережеві логи та дані, отримані з DLP-систем. Комісія проводить опитування постраждалого, підозрюваного та свідків для вивчення обставин події. У сучасних умовах до розслідувань можуть залучатися автоматизовані системи моніторингу, які використовують алгоритми машинного навчання для виявлення аномальної поведінки співробітників або підозрілих дій. Комісія також має право ініціювати технічні аудити, наприклад, аналіз безпечності мережі чи відповідності політик інформаційної безпеки. Дані, зібрані з систем аудиту, повинні бути документовані відповідно до внутрішніх стандартів організації для формування доказової бази.

Усі співробітники зобов'язані сприяти у проведенні розслідування та відповідати на всі, що належать до справи питання прямо і відверто, незалежно від того, обвинувачені вони чи свідки. Відмова відповідати на запитання та сприяти розслідуванню розцінюється як порушення субординації, яке може призвести до дисциплінарне покарання.

Затримання співробітника у приміщенні на тривалий час проти його волі під загрозою застосування сили або арешту на підставі не цілком достатніх доказів є незаконним і може викликати наступний позов про навмисне заподіяння моральної шкоди.

Якщо комісія не компетентна, визначити ступінь провини підозрюваного, до розслідування може бути залучено зовнішніх консультантів.

На останньому етапі - прийняття рішення за результатами розслідування комісія надає керівнику організації висновок про результати розслідування, в якому мають бути відображено:

- винний чи ні підозрюваний у порушенні, через яке було проведено розслідування;

- реальні наслідки, що виникли внаслідок порушення;
- потенційні наслідки, яких могло призвести порушення;
- знав чи ні підозрюваний про потенційні наслідки свого порушення;
- чи був у підозрюваного намір.

На підставі висновків комісії керівник організації може:

- не реагувати на провину, визнавши підозрюваного невинним;
- провести роз'яснювальну бесіду зі співробітником;
- винести усне чи письмове попередження;
- направити матеріали до правових органів;
- тимчасово усунути від роботи;
- звільнити з відповідних підстав.

До екстраординарної дисциплінарної санкції належить звільнення без попередження та без виплати вихідної допомоги. Така санкція застосовується до вельми серйозним порушенням, таким, як крадіжка, обман, фальсифікація документів, розголошення конфіденційної інформації, відмова виконувати законне розпорядження керівника, насильницькі дії проти товаришів по службі, прийняття хабарів від клієнтів організації тощо. Протягом п'яти днів працівник, щодо якого винесено рішення за наслідками розслідування, має право подати апеляцію з ім'ям керівника організації. Його рішення письмово повідомляється працівнику. Це рішення завершує процедуру розслідування.

З метою профілактики майбутніх порушень результати розслідування можуть бути доведені до працівників, при цьому дані учасників розслідування мають бути знеособлені

Проведений аналіз етапів проведення службових розслідувань інцидентів дозволяє сформувати вимоги до DLP систем:

- централізоване управління;
- контроль доступу до робочих станцій, мобільних пристроїв;
- контроль мережевих комунікацій;

- аналіз, фільтрація та виявлення несанкціонованого вмісту;
- контроль обміну даними;
- тіньове копіювання;
- сповіщення про нештатні ситуації;
- виявлення та блокування порушення.

На основі представленої інформації можна зробити висновки про місце DLP-систем у проведенні службових розслідувань інцидентів інформаційної безпеки. Робота систем спрямована на запобігання збору інформації співробітниками організації та відстеження спроб здійснення несанкціонованого доступу. Під час розслідування інцидентів можливості DLP-систем дозволяють створити доказову базу для подальшого розгляду, аналізу та підсумків.

2.2. Обґрунтування вибору DLP для розслідування інцидентів

Як відомо, повністю виключити ризики витоків інформації неможливо, тому розглянемо можливості DLP-систем для їх мінімізації. Системи, що побудовані на базі моніторингу додатків, знімків екрану, клавіатури розглядатись не будуть тому, що вони не вирішують ключове завдання, як би їх розробники не позиціонували на ринку. Дані системи вирішують ключове завдання – попередження витоку конфіденційних даних, а також можуть бути використані в якості інструментів вирішення інших задач з пасивним спостереженням. Для вирішення задачі було обрано:

- Symantec DLP;
- DeviceLock DLP;
- McAfee DLP;
- Sophos;
- Solar Dozor;
- Forcepoint DLP.

Розглядалися заявлені функцій систем та їх можливості виявлення спроби передачі наступних даних:

- багаторівневий архів із зміненим розширенням, з файлом *.xlsx розміром 50Мб, де цільовий текст був захований серед комірок спаму, передбачається спрацювання за заданими словами, номерами телефонів та адресами електронної пошти;
- сканований документ з двох сторінок, обернений на 180°, передбачається спрацювання на серійний номер документів;
- текстовий документ - заповнений договір, шаблон якого попередньо завантажувався в систему.

Solar Dozor є прикладом сучасної DLP-системи, яка поєднує інструменти моніторингу комунікацій, аналітики активності співробітників і механізми виявлення корпоративного шахрайства. Ця система забезпечує контроль як локальних, так і хмарних ресурсів, надаючи детальну інформацію для службових розслідувань. (рисунок 2.4).

У 2023 році багато DLP-рішень, включаючи Solar Dozor, отримали підтримку технологій машинного навчання (ML) для вдосконалення виявлення аномалій у поведінці користувачів. Наприклад, вони можуть автоматично визначати потенційно небезпечні дії, такі як масове копіювання даних, нестандартне використання корпоративних пристроїв або завантаження файлів у незахищені хмарні сховища.

Forcepoint DLP забезпечує інтеграцію з корпоративними хмарними сервісами, такими як Microsoft 365 або Google Workspace, що дозволяє ефективно контролювати дані у віддалених середовищах. Symantec DLP розширила свої функції, включивши аналіз немережею комунікацій, таких як USB-пристрої чи локальний друк, а також підтримку хмарних середовищ із застосуванням Zero Trust підходу.

Вибір DLP-системи для службових розслідувань залежить від кількох факторів:

- підтримка багатоканального моніторингу (локальні та хмарні ресурси);
- можливість інтеграції з SIEM-системами для комплексного аналізу;
- використання поведінкової аналітики для виявлення аномалій;
- наявність модулів автоматичного створення доказової бази (логів, знімків екрану тощо).

Сучасні DLP-системи відіграють критичну роль у проведенні службових розслідувань, забезпечуючи прозорість дій користувачів та допомагаючи швидко реагувати на інциденти. Їх використання дозволяє ефективно виявляти загрози, документувати їх, а також запобігати подібним ситуаціям у майбутньому [15].

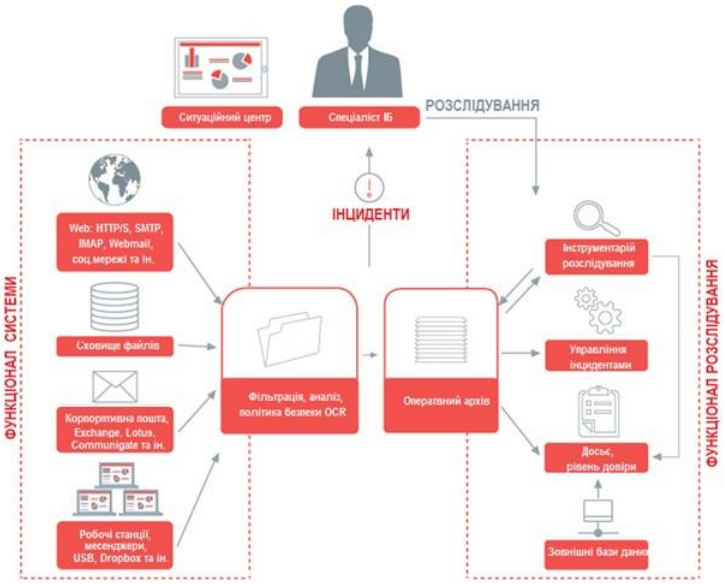

Рисунок 2.1 – Інструментарій розслідування інцидентів

Основний акцент - аналітичні можливості. На сайті розробника заявлено, що модульна архітектура системи дозволяє розподілити навантаження та розгорнути її на будь-якому ПК. Для її використання необхідні технічні навики. Приклад інтерфейсу Solar Dozor наведений на рисунку 2.2.

Рисунок 2.2 – Робочий стіл Solar Dozor

Проте за документацією необхідно виділити сервер з 8-ми ядерним процесором та 32Гб пам'яті для того, щоб забезпечити запуск мінімальної конфігурації. Також необхідно встановити додатковий проксі та поштовий сервер. Дана система має високі технічні вимоги [16].

Forcepoint DLP передбачає захист від витоку даних. Дозволяє розширити засоби контролю інформації на корпоративних хмарних ресурсах та кінцевих пристроях. Це дозволяє безпечно використовувати такі сервіси, як Microsoft Office 365, Google for Work та SalesForce.com, а також захищати конфіденційність даних й інтелектуальну власність на портативних комп'ютерах Mac та Windows як у мережі, так і поза нею [17]. На рисунку 2.3 наведена будова системи.

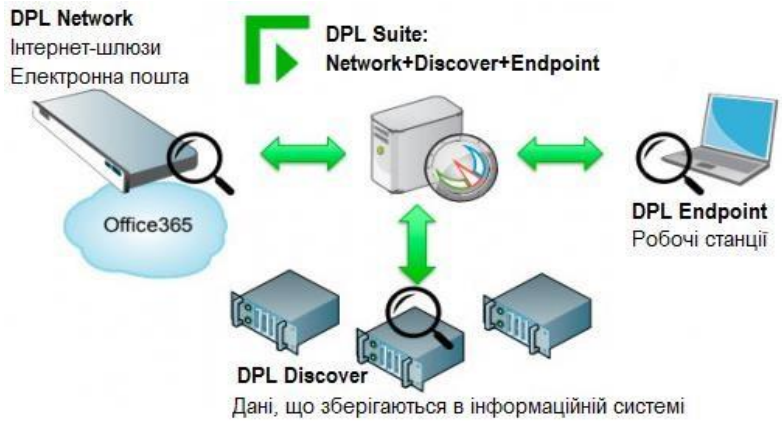

Рисунок 2.3 - Компоненти Forcepoint DLP

Контроль даних для їх захисту відбувається незалежно від того, зберігаються вони чи виконується їх обробка. На рисунку 2.4 наведений приклад вікна програми [18].

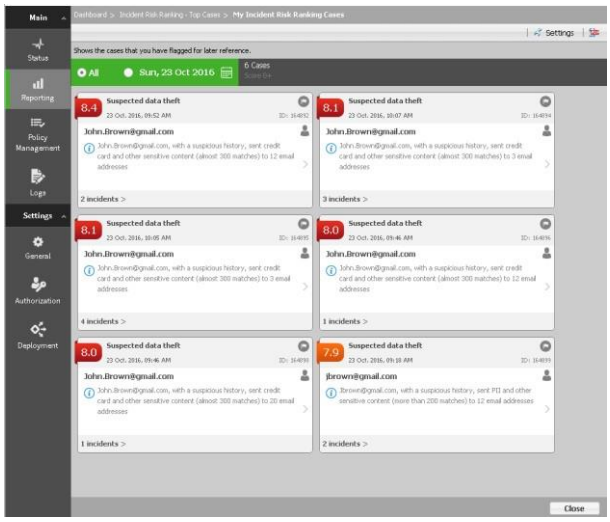

Рисунок 2.4 - Інтерфейс Forcepoint DLP

Система Forcepoint проста у використанні, характеризується невеликим числом помилкових спрацьовувань та тривог.

Symantec DLP – система має не модульну архітектуру, як наведена на рисунку 2.5, забезпечує запобігання витоку даних та дозволяє вирішити проблему захисту інформації для неструктурованих даних [19].

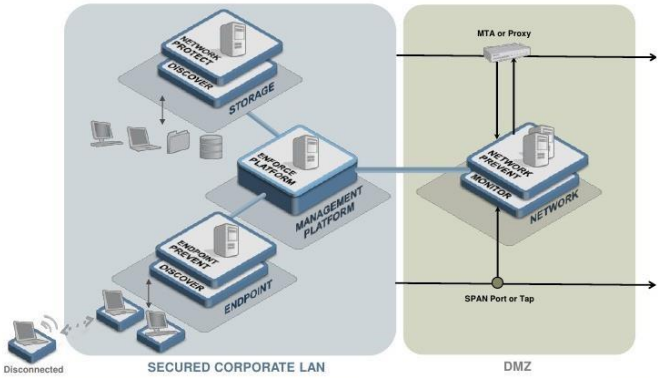

Рисунок 2.5 – Архітектура Symantec DLP

Symantec DLP за допомогою комплексного підходу до захисту інформації, який охоплює сучасні хмарні та мобільні технології, дозволяє визначати сховища де зберігаються дані: хмарні, мобільні, мережеві, кінцеві

точки чи системи зберігання, слідкувати за тим, як використовуються дані, чи підключені ваші співробітники до мережі чи вимкнені та здійснювати захист даних від витоку чи крадіжки — незалежно від того, де вони зберігаються та як використовуються [20]. Приклад вікна наведений на рисунку 2.6.

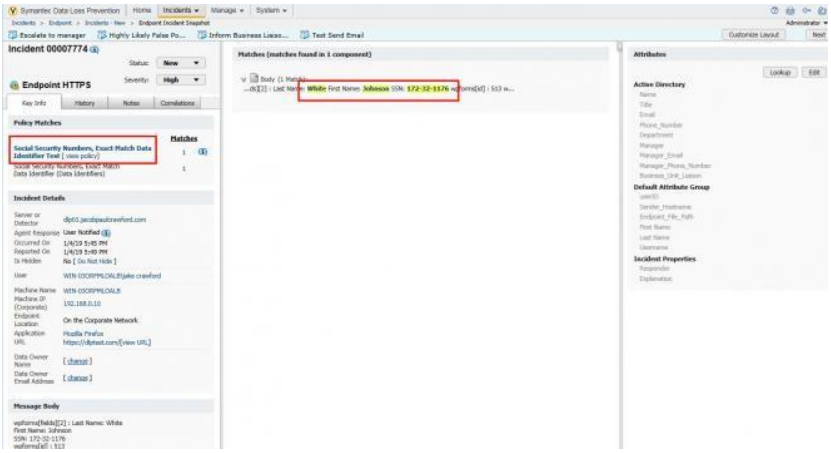

Рисунок 2.6 – Робочий стіл Symantec DLP

Symantec характеризується функціональними можливостями виявлення даних, моніторингу та захисту для GDPR, PCI, HIPAA та SOX., а також забезпечує захист даних від відомих загроз і обмежує підозрілі програми.

McAfee DLP (рисунок 2.7) дозволяє ідентифікувати та захищати дані в мережі, допомагає розуміти, які типи даних є в мережі, як здійснюється доступ до них і як вони передаються, а також містять дані про важливу або конфіденційну інформацію. Рішення McAfee DLP може використовуватися для створення та впровадження ефективної політики безпеки, зменшуючи кількість спроб та помилок [21].

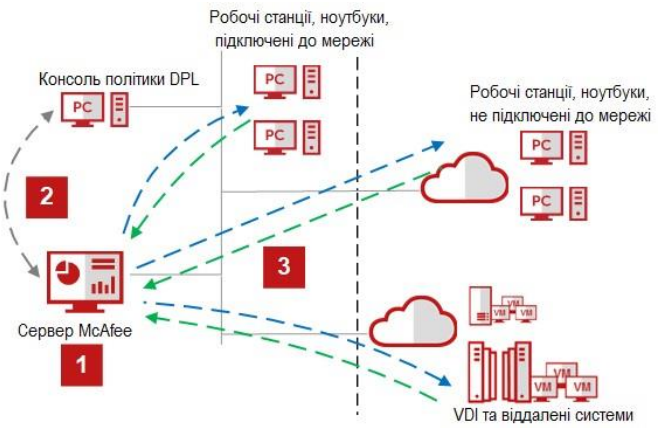

Рисунок 2.7 – Архітектура McAfee DLP

Система має функції розширеного захисту використання технології ідентифікації вмісту за його відбитками, класифікації та механізму призначення тегів для забезпечення захисту конфіденційних неструктурованих даних, таких як інтелектуальна власність та комерційна таємниця [22].

Система забезпечує захист по всіх каналах потенційного витоку даних, включаючи знімні пристрої, хмарні служби, повідомлення електронної пошти, засоби обміну миттєвими повідомленнями, веб-завантаження, засоби друку, буфер обміну, знімки екрана і програми для обміну файлами (рисунок 2.8).

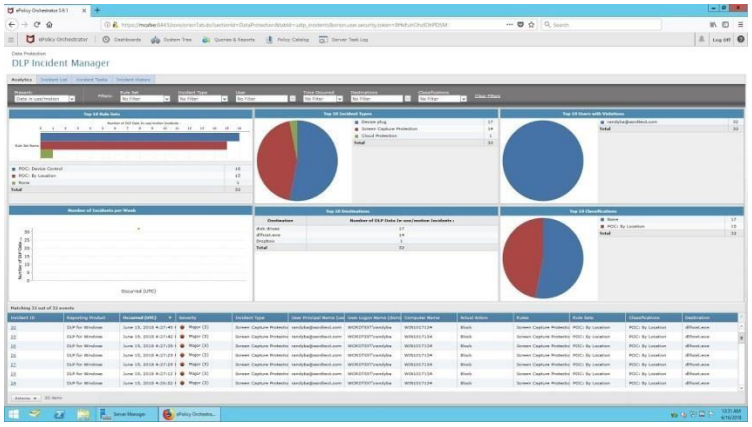

Рисунок 2.8 – Вікно McAfee DLP

McAfee DLP забезпечує централізоване керування інцидентами та отримання звітів та дозволяє синхронізувати локальні та хмарні політики DLP.

Sophos дозволяє забезпечити повну безпеку, що включає шифрування, веб-фільтрацію і patch assessment, містить інструменти, щоб зупинити шкідливі програми та захистити дані з однієї консолі за допомогою агента [23]. Архітектура системи наведена на рисунку 2.9.

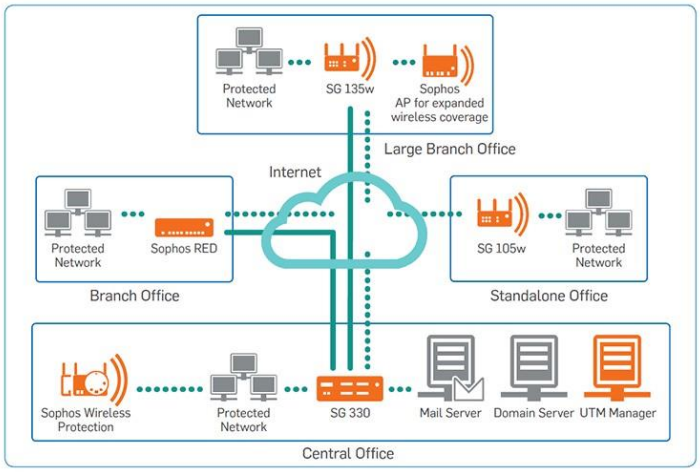

Рисунок 2.9 - Архітектура системи Sophos

Sophos, легко управляється з однієї консолі, включаючи patch assessment та веб-фільтрацію. Налаштування правил виявлення, безкоштовні оновлення безпеки та оновлення програмного забезпечення, забезпечують зручне використання. Забезпечує захист конфіденційних даних від випадкового чи навмисного викриття за допомогою знімних пристроїв, Інтернет-програм або електронної пошти [24]. Приклад консолі системи наведений на рисунку 2.10.

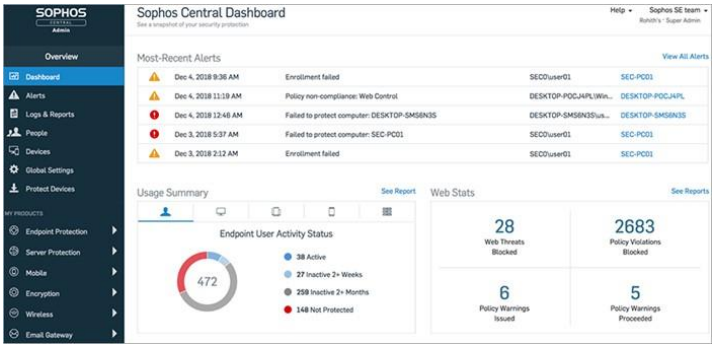

Рисунок 2.10 - Вікно Sophos

Sophos – це ефективний та простий інструмент захисту даних який не вимагає встановлення додаткового програмного забезпечення.

DeviceLock DLP Suite включаєз взаємодоповнюючі функціональні модулі

- DeviceLock, NetworkLock, ContentLock, DeviceLock Discovery та DeviceLock Search Server (DLSS), які ліцензуються в будь-яких комбінаціях для вирішення задач служб ІБ (рисунок 2.11) [25].

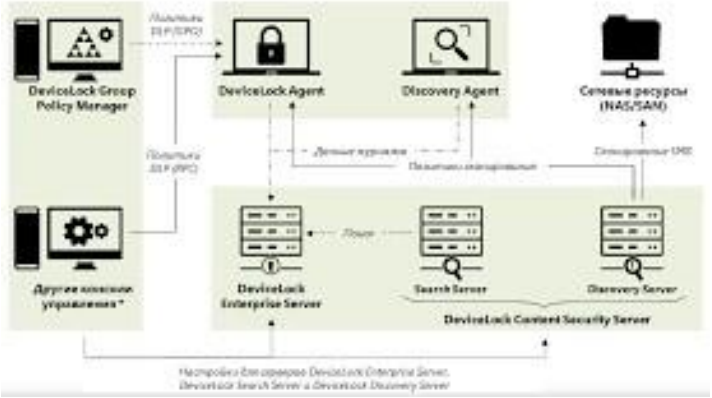

Рисунок 2.11 – Структурні компоненти DeviceLock

DeviceLock дозволяє керувати доступом користувачів до пристроїв через групову політику домену При використанні програмних та апаратних засобів шифрування даних, DLP дозволяє службам ІБ централізовано віддалено керувати політиками шифрування, що забезпечують гарантоване використання співробітниками криптографічних засобів при зберіганні та переносі даних на знімних носіях. Приклад інтерфейсу системи наведений на рисунку 2.12.

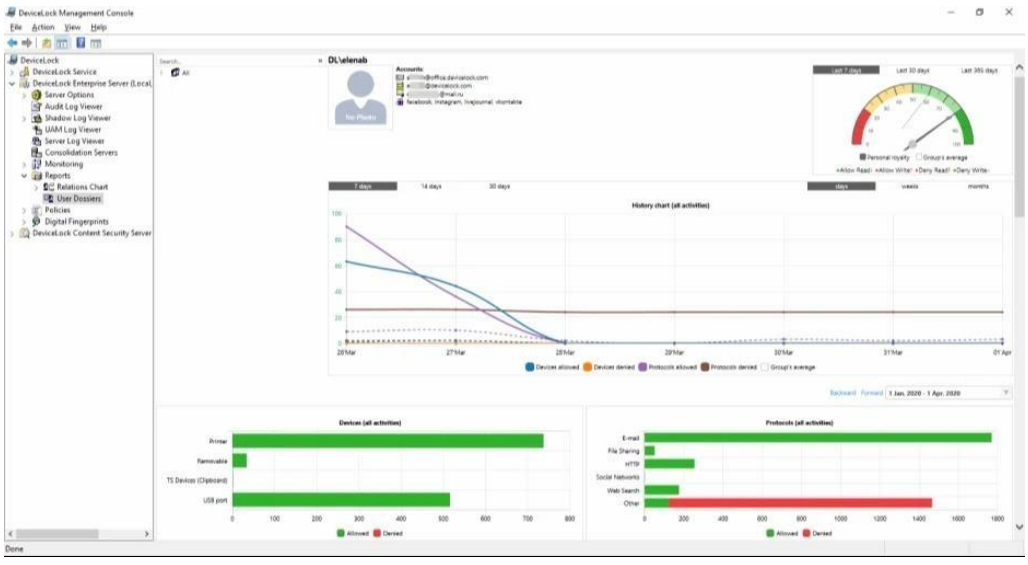

Рисунок 2.12 – Робоче вікно DeviceLock DLP

DeviceLock DLP забезпечує можливість найвищого рівня контролю пристроїв та мережевих протоколів, що не забезпечується стандартними засобами групових політик Windows. Дана можливість реалізується за допомогою інтерфейсу, що прозоро інтегрується в редактор групових політик Windows Group Policy Editor та дозволяє легко керувати контролем доступу у великих корпоративних мережах [26].

Таблиці 2.1 - 2.4 ілюструють можливості розглянутих систем попередження витоку даних.

Таблиця 2.1 – Характеристики DLP-систем для блокування пристроїв

Параметр / DLP-система	Флешнакописувач	Локальний USB принтер	Мережевий принтер
McAfee	+	+	+
Sophos	+	-	-
Symantec	+	+	+
DeviceLock	+	+	+
Solar Dozor	+	+	+
Forcepoint	+	-	-

Таблиця 2.2 – Характеристики DLP-систем щодо блокування даних

Параметр / DLP-система	Мережеві канали	Термінальна сесія	Вміст
McAfee	+	+	+
Sophos	-	-	+/-
Symantec	+/-	+/-	-
DeviceLock	+	+	+
Solar Dozor	+/-	+	-
Forcepoint	+/-	+	-

Таблиця 2.3 – Характкристики DLP-систем щодо заборони надсилання файлів

Параметр / DLP-система	Архів	Скановані документи	Текстовий документ
McAfee	+	-	+/-
Sophos	-	-	-
Symantec	-	-	-
DeviceLock	+	+	+
Solar Dozor	-	-	-
Forcepoint	-	-	-

Таблиця 2.4 – Характеристики DLP-систем

Параметр / DLP-система	Сповіщення	Тіньові копії
McAfee	від сервера	+
Sophos	від агента	-
Symantec	від сервера	+/-
DeviceLock	від агента	+
Solar Dozor	від сервера	+
Forcepoint	від сервера	+

З таблиць видно, що найкращі характеристики має DeviceLock DLP. Перевагою системи є деталізація у налаштуваннях контролю. Наприклад, контроль Viber включає не лише події, тіньові копії, сповіщення, перевірку вмісту, а й- контроль окремих складових Viber - чат, файли, дзвінки. Список контрольованих пристроїв і мережевих каналів побудований зручно та достатньо великий. Є вбудований OCR модуль. Блокування вмісту працюють,

хоча з деяким навантаженням на робочі станції. Сповіщення можуть приходити майже миттєво. Агенти незалежні від серверної частини, можуть працювати автономно очікуючи підключення.

Недоліком є відсутність майстра політики. Передбачається покрокове створення політики, тобто для налаштування будь-якої політики необхідно на початку розуміти, що необхідно отримати, та у відповідних розділах консолі відмічати параметри, вибирати користувачів та ін. З іншого боку, це дозволяє перевірити, що задане у плані контролю. Пошук архіву обмежений повнотекстовим пошуком за вмістом тіньових копій. Немає можливості пошукати за шаблоном документу або за допомогою словників. Система має розвинену систему фільтрів, але це не контентні фільтри. Під час роботи контентно-залежних правил неминучим є навантаження на робочі станції.

Реалізовано автоматичне перемикання режимів – співробітника з ноутбуком може переміщуватися а, політики перемикатимуться самі на інші налаштування. Блокування та моніторинг у системі розділені на рівні консолі, тому немає жодних перешкод налаштувати для певних каналів заборону для окремих співробітників, а іншим задати налаштування лише для моніторингу. Також самостійними є правила аналізу вмісту. Вони працюють як на заборону, так і на дозвіл передачі при закритому каналі.

2.3. Засоби підвищення стійкості DLP систем

DLP системи забезпечують можливість дізнатися, з якої робочої станції та облікового запису зроблена спроба порушення ІБ, проте визначити самого порушника не вийде, оскільки, існує можливість входу в систему іншої людини під обліковим записом легального користувача.

Пропонується розширити можливості систем за рахунок використання веб-камер. Це дозволить створити доказову базу для розслідування інцидентів, за яких здійснювався фізичний доступ до робочої станції.

База параметрів для розпізнавання облич всіх користувачів створюється перед початком експлуатації та знаходиться на сервері, а на локальних машинах – лише суб'єктів, мають доступ до даної робочої станції. Визначення особи користувача проводиться із заданою періодичністю. Спрощена схема алгоритму роботи запропонованої технології представлена рисунку 2.13.

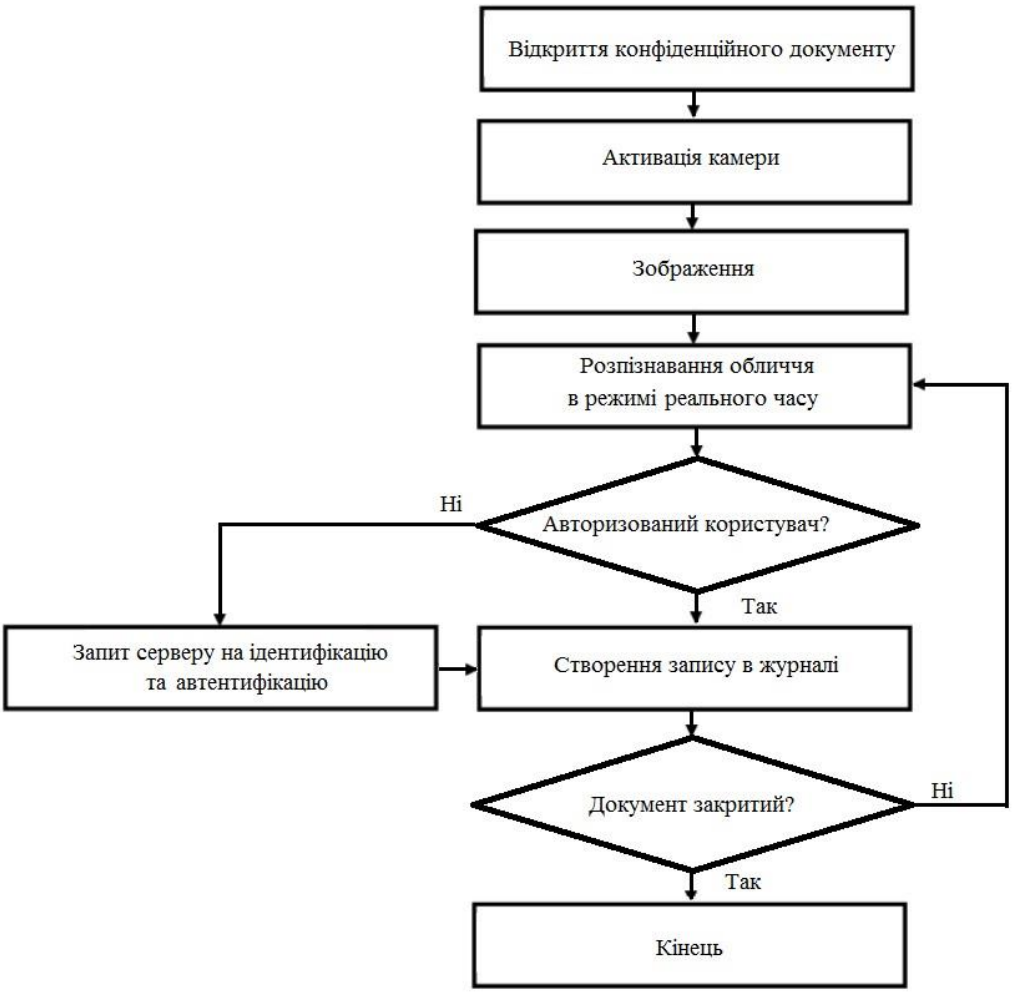

Рисунок 2.13 - Схема алгоритму захисту від несанкціонованого доступу до інформації

Алгоритм роботи запропонованої технології наступний.

Крок 1. При відкритті користувачем конфіденційного документа здійснюється активація веб-камери та проводиться знімок для подальшого розміщення в журнал аудиту.

Крок 2. За допомогою камери виділяється особа користувача та проводиться збір значень для визначення особи.

Крок 3. Отримані значення порівнюються з еталонними, що зберігаються на локальній машині, якщо користувач не знайдений у локальній базі, тоді серверу надсилається запит на ідентифікацію та автентифікацію користувача. У тому випадку, якщо значення не відповідають ні одному з еталонних, ім'я користувача передається як «невизначений». Якщо користувач знайдений у локальній На основі, цей крок пропускається.

Крок 4. Після визначення особи користувача створюється запис у журналі аудиту наступного змісту: час; повне ім'я документа; робоча станція; програма, у якій відкрито документ; Ім'я користувача, знімок.

Крок 5. Якщо через заданий проміжок часу документ не закрито, здійснюється перехід на другий крок, а якщо документ закрито, тоді завершується робота механізму до наступного відкриття документа конфіденційного характеру. Технологія захисту за даним алгоритмом має працювати у прихованому режимі, щоб запобігти спробам протидії з боку користувачів.

2.4. Висновки до розділу

1) Проаналізовано етапи проведення службових розслідувань інцидентів, що дозволило сформувати вимоги до DLP-системи, використання якої забезпечить управління інформаційною безпекою.

2) Проаналізовано сучасні інструментальні засоби контролю та захисту від витоку конфіденційної інформації. Зроблено вибір DLP-системи, яка володіє необхідним інструментарієм та забезпечує виконання оптимального характеристики та функції для реалізації управління інцидентами інформаційної безпеки.

3) Запропоновано алгоритм захисту від несанкціонованого доступу до інформації, що дозволяє підвищити стійкість обраної DLP системи.

3. Встановлення та розгортання dlp-системи

3.1. Компоненти DLP-системи DeviceLock

До складу програмного комплексу DeviceLock DLP входять три основні частини:

- агент (сервіс DeviceLock),
- сервери (DeviceLock Enterprise Server та DeviceLock Content Security Server)
- консолі управління (DeviceLock Management Console, DeviceLock Group Policy Manager та DeviceLock Enterprise Manager).

Схема роботи сервісу наведена на рисунку 3.1.

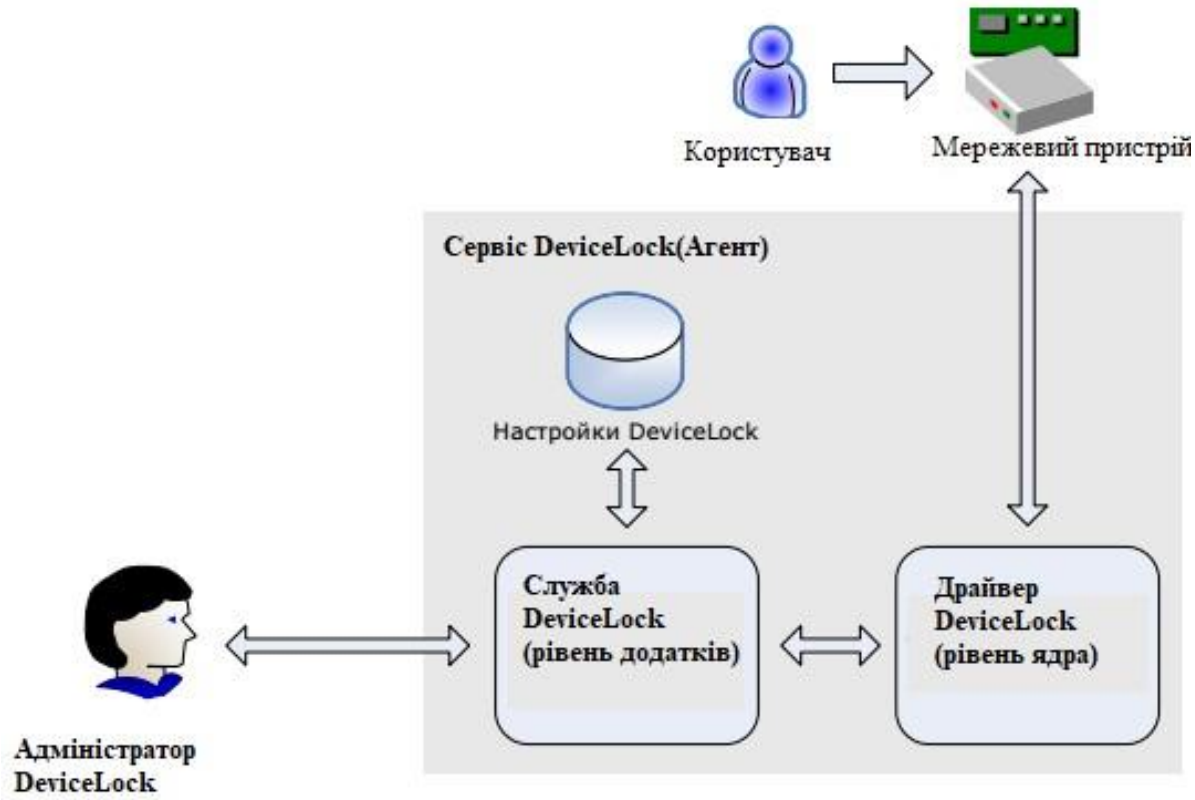

Рисунок 3.1 Схема роботи системи

Агент DeviceLock, або сервіс DeviceLock – це ядро системи DeviceLock. Агент встановлюється на кожен контрольований комп'ютер, автоматично запускається та забезпечує захист пристроїв та мережі на машині-клієнті, залишаючись у той же час невидимий для локального користувача.

DeviceLock Enterprise Server (DLES) – це додатковий компонент, призначений для централізованого збирання та зберігання даних тіньового копіювання та журналів аудиту. Для зберігання даних DeviceLock Enterprise Server використовує сервер бази даних - SQL Server або PostgreSQL. Для рівномірного розподілу навантаження в локальної мережі можна встановити кілька екземплярів DLES та серверів бази даних.

DeviceLock Content Security Server – ще один додатковий компонент, що включає компонент Search Server для швидкого пошуку тексту у файлах тіньового копіювання та журнали, що зберігаються на DeviceLock Enterprise Server.

Схема взаємодії серверів та клієнтів DLP наведена на рисунку 3.2.

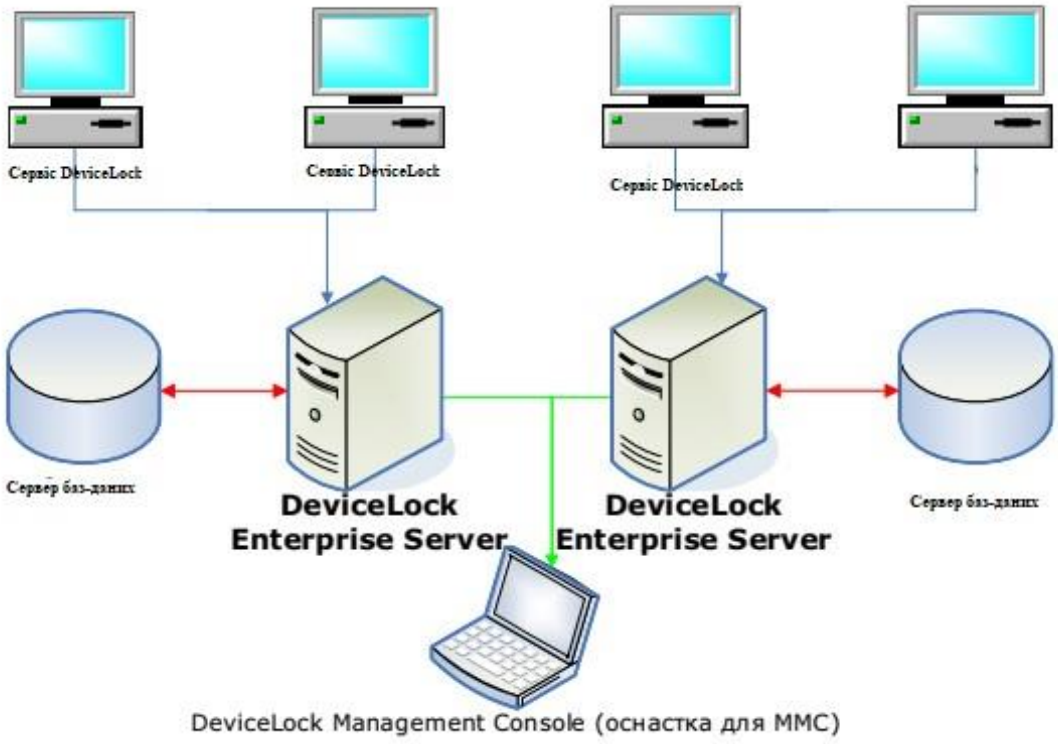

Рисунок 3.2 - Схема взаємодії серверів та клієнтів DLP

Консоль управління – це інтерфейс контролю, який системний адміністратор використовує для віддаленого керування будь-якою системою, де встановлено сервіс DeviceLock (рисунок 3.3). DeviceLock поставляється з чотирма консолями управління: DeviceLock Management Console, DeviceLock Enterprise Manager та DeviceLock Group Policy Manager (Інтегрується в редактор групових політик Windows). DeviceLock Management Console також використовується для керування серверами DeviceLock Enterprise Server та Content Security Server.

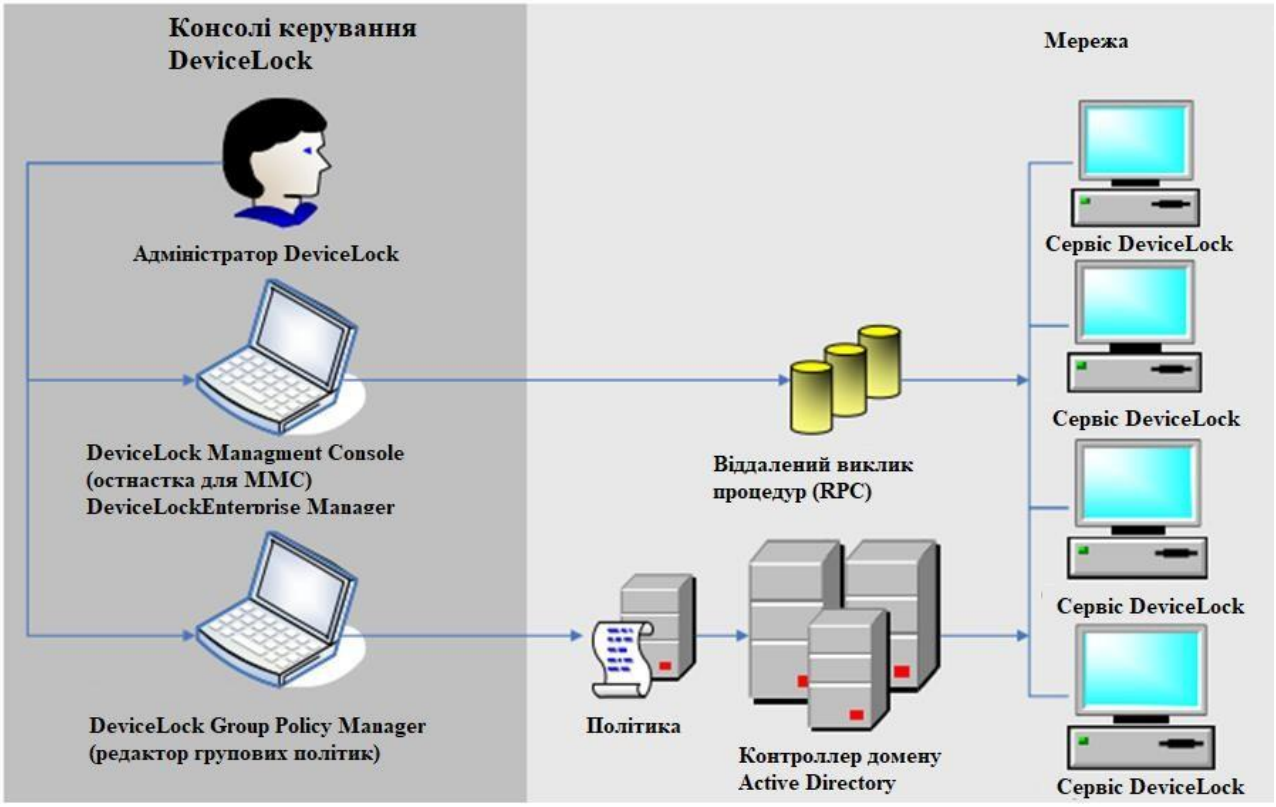

Рисунок 3.3 – Консолі управління DeviceLock

До складу програмного комплексу DeviceLock DLP входять сервіс DeviceLock, сервер DeviceLock Enterprise Server, сервер DeviceLock Content Security Server, а також консолі керування DeviceLock Management Console, DeviceLock Group Policy Manager та DeviceLock Enterprise Manager. Нижче наводяться системні вимоги щодо кожного з цих компонентів.

3.2. Керований контроль доступу

Контроль доступу для пристроїв працює наступним чином: щоразу, коли користувач намагається отримати доступ до пристрою, DeviceLock перехоплює запит на рівні ядра ОС. Залежно від типу пристрою та інтерфейсу підключення (наприклад, USB), DeviceLock перевіряє права користувача у відповідному списку управління доступом (ACL). Якщо користувач не має права доступу до цього пристрою, буде повернено повідомлення про помилку "доступ заборонено". Схема доступу до файлу наведена на рисунку 3.4.

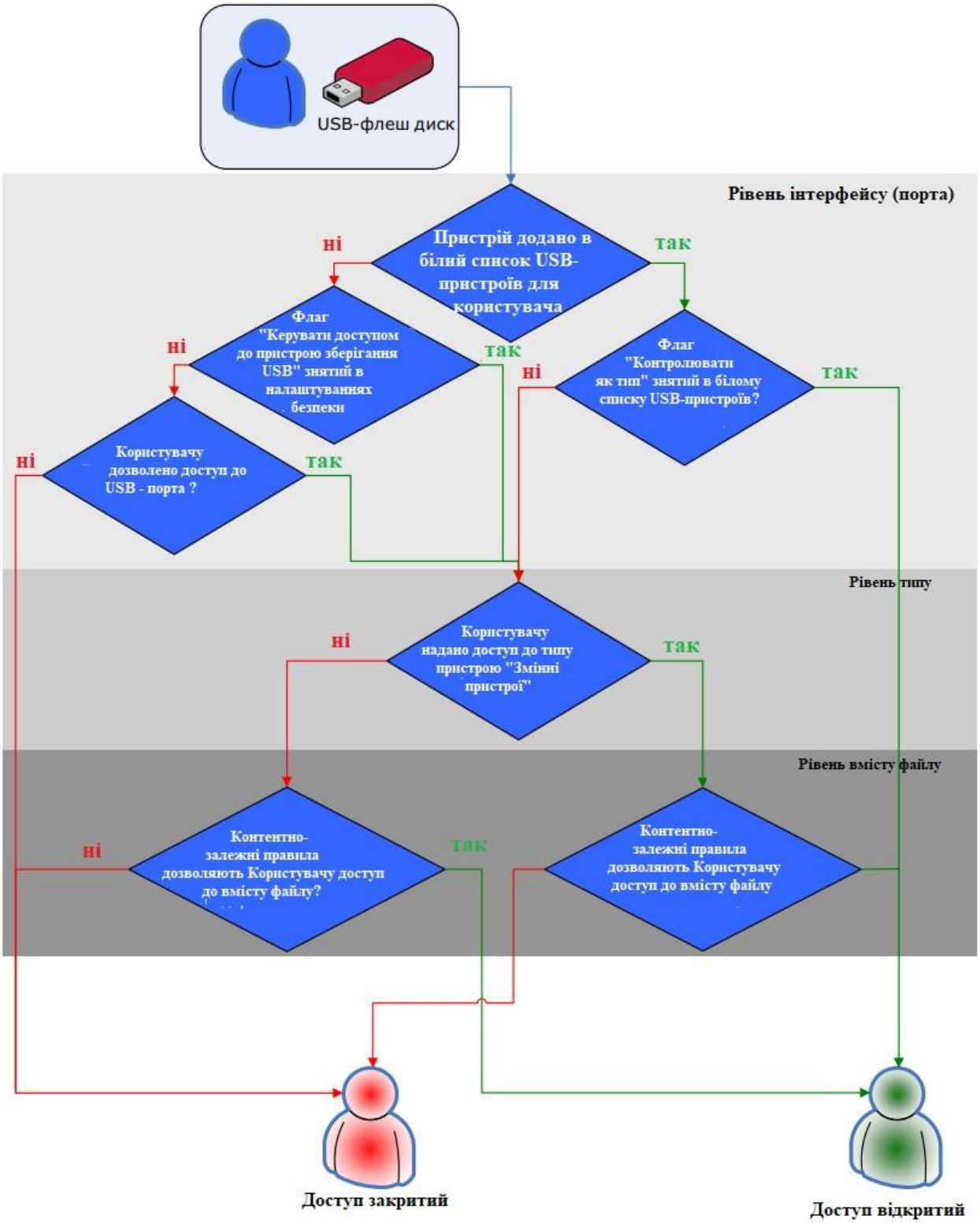

Рисунок 3.4 – Схема доступу до файлу

Перевірка дозволів на доступ виконується на трьох рівнях: інтерфейс (порт), тип та вміст файлу. Деякі пристрої перевіряються на всіх трьох рівнях, тоді як інші - тільки одному: або лише на рівні інтерфейсу (порту), або лише на рівні типу.

Розглянемо нагоду доступу користувача до USB-флеш через USB-порт. В даному випадку DeviceLock насамперед перевірить на рівні інтерфейсу (USB-порту), відкритий чи ні доступ до USB-порту. Потім, оскільки Windows визначає USB-флеш як знімний пристрій, DeviceLock також перевірить обмеження на рівні типу пристрою (знімне). І на завершення перевірки DeviceLock також перевірить обмеження на рівні вмісту файлу, визначені контентно-залежними правилами.

У разі використання USB-сканера доступ буде перевірятися лише на рівні інтерфейсу (USB-порту), оскільки DeviceLock не має окремого типу пристроїв для сканерів. Схема перевірки USB сканера наведена на рисунку 3.5.

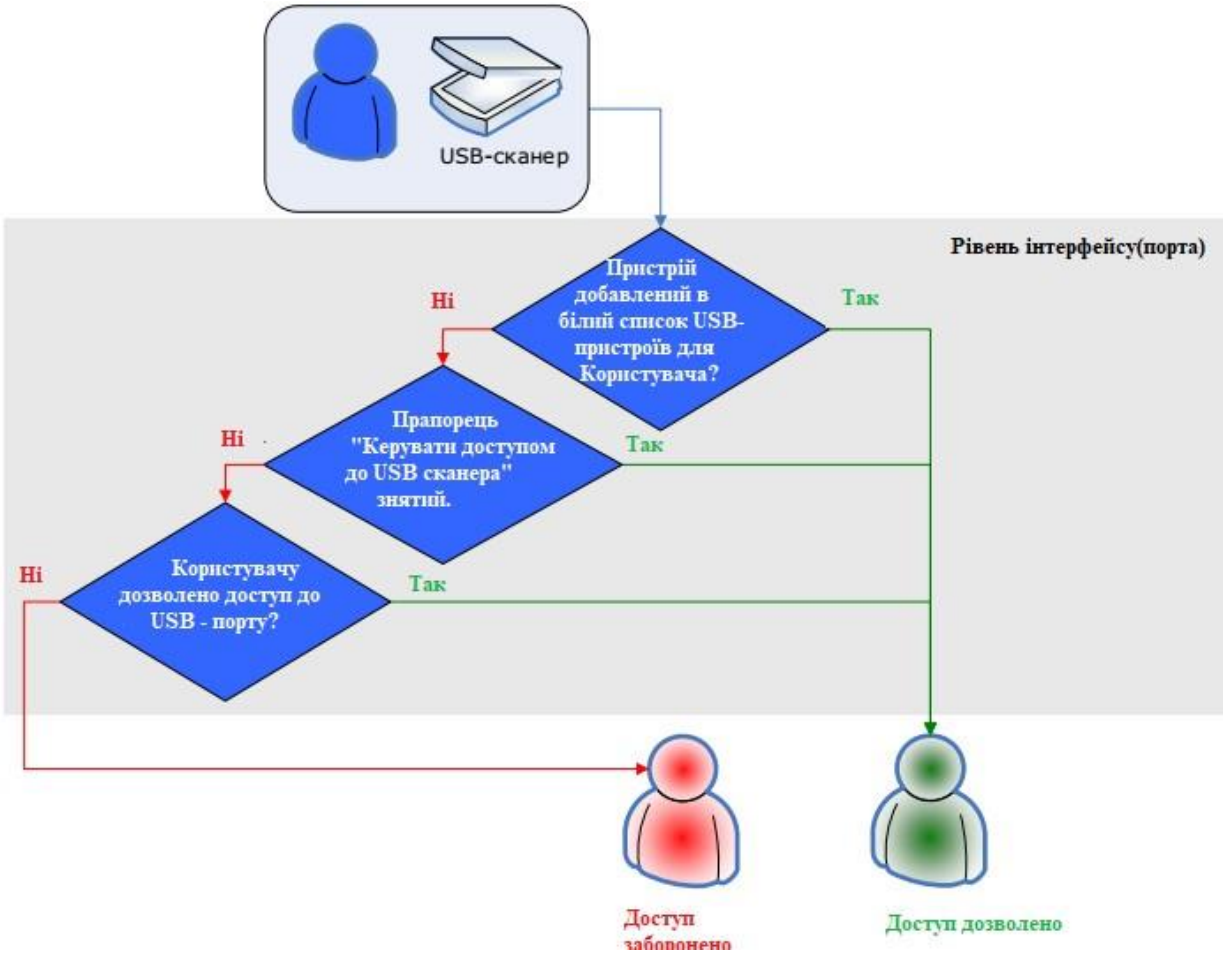

Рисунок 3.5 – Схема перевірки USB сканера

Існують додаткові параметри безпеки. Налаштування безпеки (звичайний профіль), які можуть вимикати контроль доступу для класів пристроїв, наприклад, для всіх USB-клавіатур і мишей, у той час як інші

пристрої залишаються під контролем. В у випадку, якщо пристрій належить до класу, для якого контроль вимкнено, DeviceLock пропускає всі запити на з'єднання з цим пристроєм на рівні інтерфейсу (порту).

DeviceLock також підтримує білий список певних пристроїв. Наприклад, білий список USB-пристроїв безпеки (звичайний профіль) дозволяє вимкнути контроль доступу лише для певних пристроїв - деяких USB-принтерів. Схема перевірки протоколів наведена на рисунку 3.6.

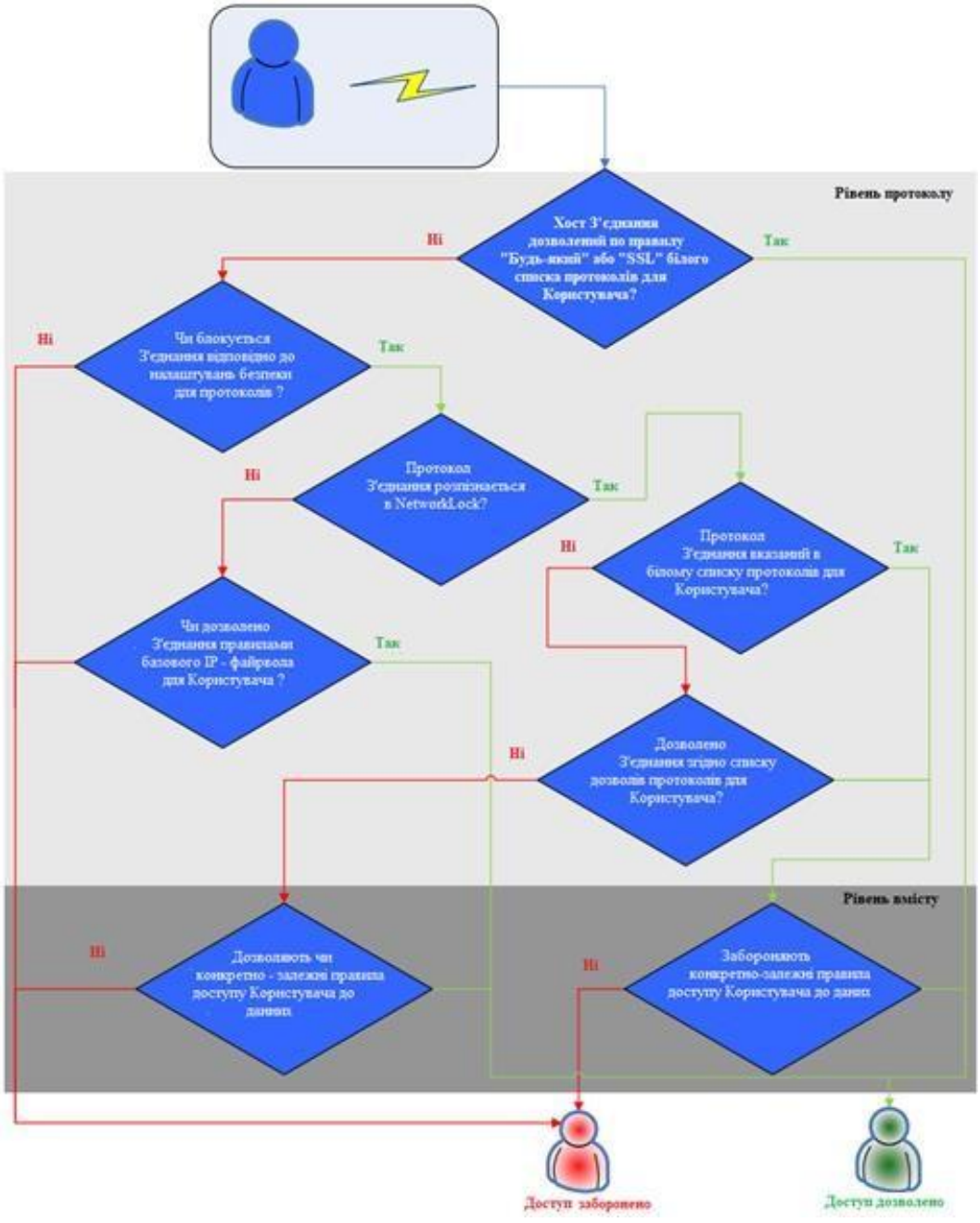

Рисунок 3.6 – Схема перевірки протоколів

Контроль доступу для протоколів працює наступним чином: щоразу, коли користувач намагається отримати доступ до віддаленого мережного ресурсу, DeviceLock перехоплює запит на з'єднання на рівні ядра ОС і перевіряє права користувача відповідному списку керування доступом (ACL)

Якщо користувач не має права доступу до цього протоколу буде повернено повідомлення про помилку “доступ заборонено”.

Перевірка дозволів на доступ виконується на двох рівнях:

- протокол;
- вміст.

Всі мережеві підключення перевіряються на обох рівнях, за винятком підключень по протоколам Торрент, Telnet, Telegram та WhatsApp, які перевіряються лише на рівні протоколу.

Наприклад, при спробі користувача підключитися до віддаленого вузла, DeviceLock перевірить, чи дозволено підключення на рівні протоколу, а потім будуть перевірені дозволи на рівні вмісту даних, що передаються, визначені контентно-залежними правилами.

Розглянемо можливість доступу користувача до сайту соціальної мережі. Дуже часто компанії забороняють своїм співробітникам користуватися месенджерами, соціальними мережами та поштовими сервісами на корпоративному брандмауері, але при цьому залишається ризик підключення комп'ютерів до мережі Інтернет, оминаючи блокування за допомогою персональних Wi-Fi-підключень або модемів для стільникових мереж. DeviceLock забезпечує контроль найбільш популярних мережевих програм та сервісів – повідомлення електронної пошти та вкладення, закачування файлів у мережу, web-пошту та соціальні мережі, служби миттєвих повідомлень та файловий обмін за протоколами FTP/FTP-SSL та HTTP/HTTPS.

Схема доступу до соціальних мереж наведена на рисунку 3.7.

У цьому випадку DeviceLock насамперед перевірить на рівні протоколу, відкритий чи ні доступ до соціальних мереж.

Потім DeviceLock перевірить дозволи на рівні вмісту даних, визначені контентно-залежними правилами.

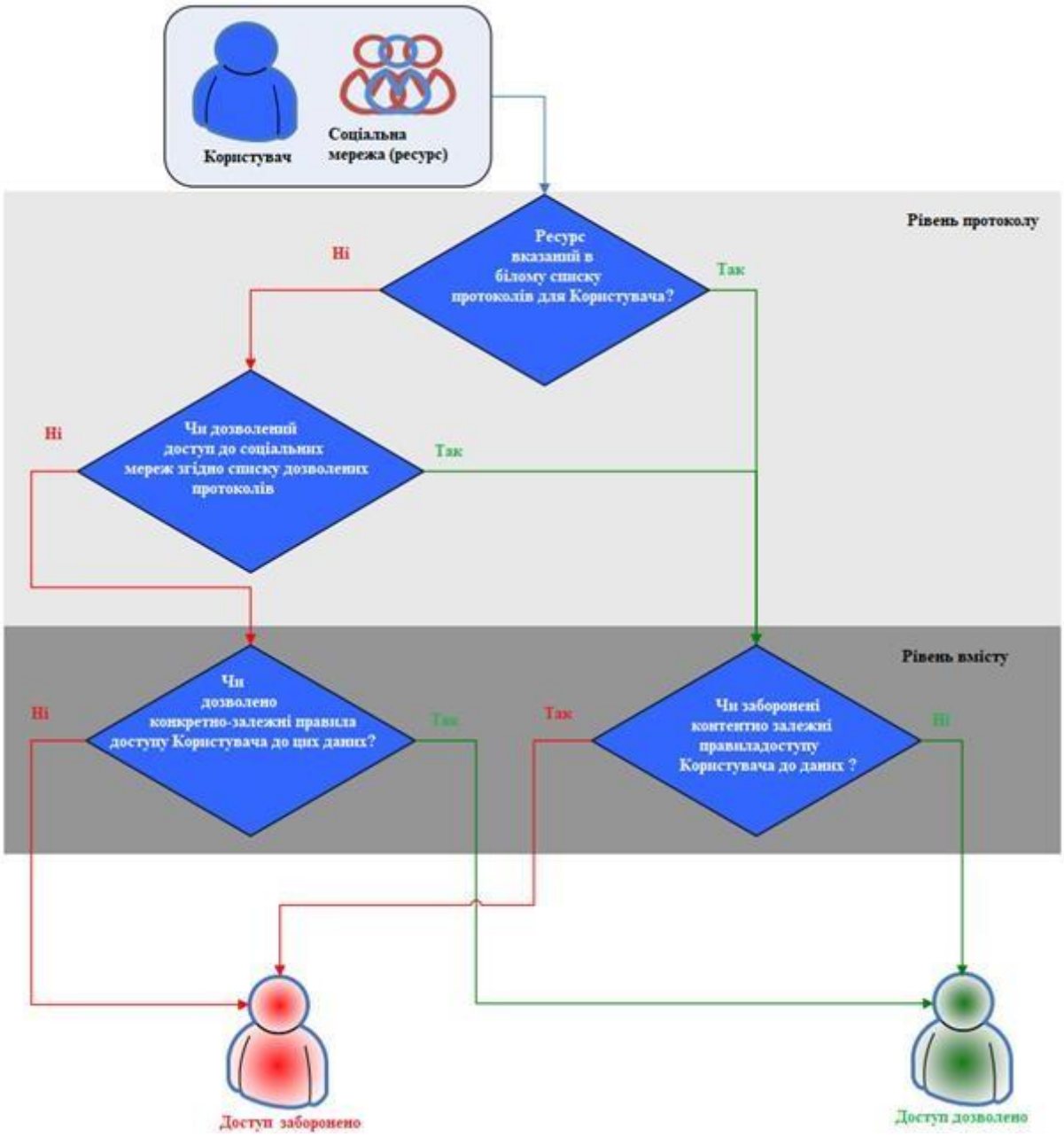

Рисунок 3.6 – Схема доступу до соціальних мереж

Крім того, DeviceLock підтримує білий список протоколів, що дозволяє вимкнути контроль доступу для мережевих підключень з певними параметрами, наприклад, HTTP-підключень для певних вузлів та портів.

3.3. Встановлення DeviceLock

Комп'ютер для встановлення сервісу DeviceLock повинен відповідати таким вимогам:

До складу програмного комплексу DeviceLock DLP входять:

- сервіс DeviceLock;
- сервери:
  - DeviceLock Enterprise Server;
  - DeviceLock Content Security Server
- консолі керування:
  - DeviceLock Management Console;
  - DeviceLock Group Policy Manager;
  - DeviceLock Enterprise Manager.

Нижче наводяться системні вимоги щодо кожного з цих компонентів.

Комп'ютер для встановлення сервісу DeviceLock повинен відповідати таким вимогам:

- ОС Windows для сервісу DeviceLock:
  - Microsoft Windows XP/Vista/7/8/8.1/10, Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 чи Windows Server 2019.
  - допускаються 32- та 64-розрядні версії операційної системи.
- ОС Mac для сервісу DeviceLock:
  - macOS 10.15 (Catalina) або macOS 11.2.3 (Big Sur).
  - пам'ять (ОЗП) Мінімум: 512 МБ.
  - вільне місце на жорсткому диску: від 400 МБ.
  - процесор мінімальна вимога: Intel Pentium 4.

Підтримувані засоби віртуалізації:

- Microsoft Remote Desktop Services;

- Citrix XenDesktop/XenApp;
- Citrix, XenServer;
- VMware Horizon View;
- VMware Workstation;
- VMware Player;
- Oracle VM VirtualBox;
- Windows Virtual PC.

Для проведення тестів проведемо встановлення DeviceLock Security Server. При встановленні буде відображено вікно з ліцензійними умовами, як це показано на рисунку 3.7.

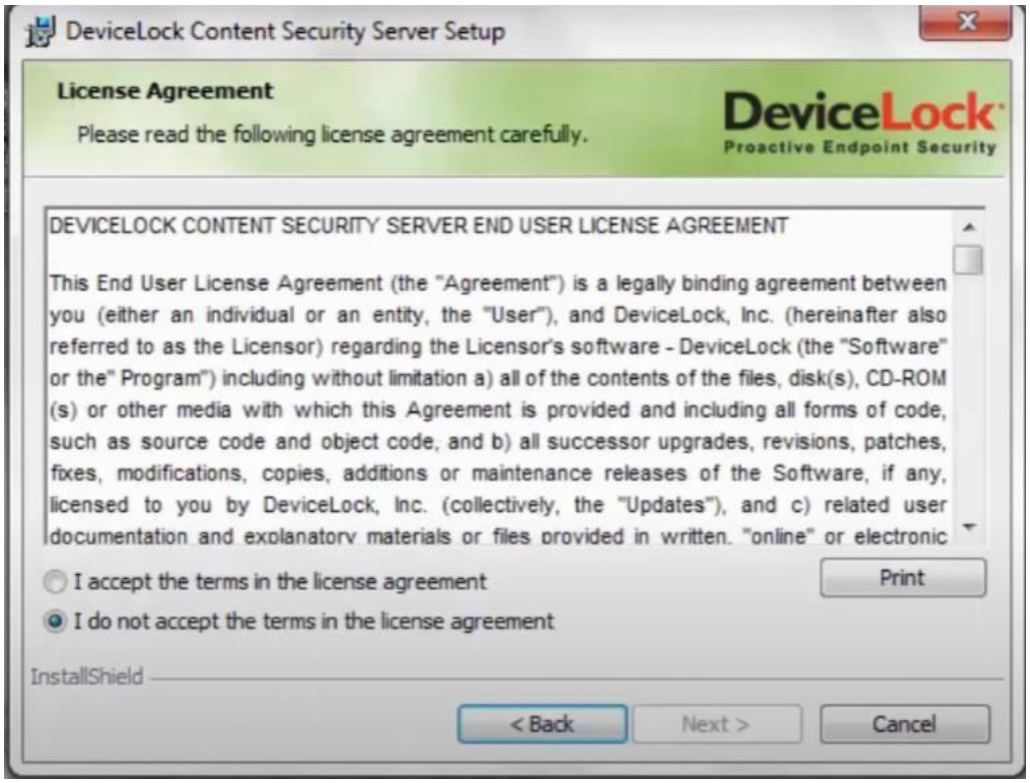

Рисунок 3.7 – Початок встановлення DeviceLock Security Server

Продукт було отримано на правах пробної ліцензії доступної протягом 30 днів. Більшість функцій в тестовому режимі будуть доступні. В процесі встановлення можна обрати від імені якого користувача буде працювати сервіс.

Щоб запустити службу під обліковим записом системи, необхідно обрати опцію - локальний обліковий запис системи. Слід пам'ятати, що програми, які працюють під цим обліковим записом, не можуть отримати доступ до мережевих ресурсів і авторизуються на віддалених комп'ютерах як анонімний непривілейований користувач. Таким чином, DeviceLock Content Security Server, запущений під локальним обліковим записом системи, не зможе отримати доступ до мережевих ресурсів, і повинен використовувати сертифікат DeviceLock для авторизації на сервері DeviceLock Enterprise Server, що працює на віддаленому комп'ютері.

Вікно початкового налаштування DeviceLock Security Server наведено на рисунку 3.8.

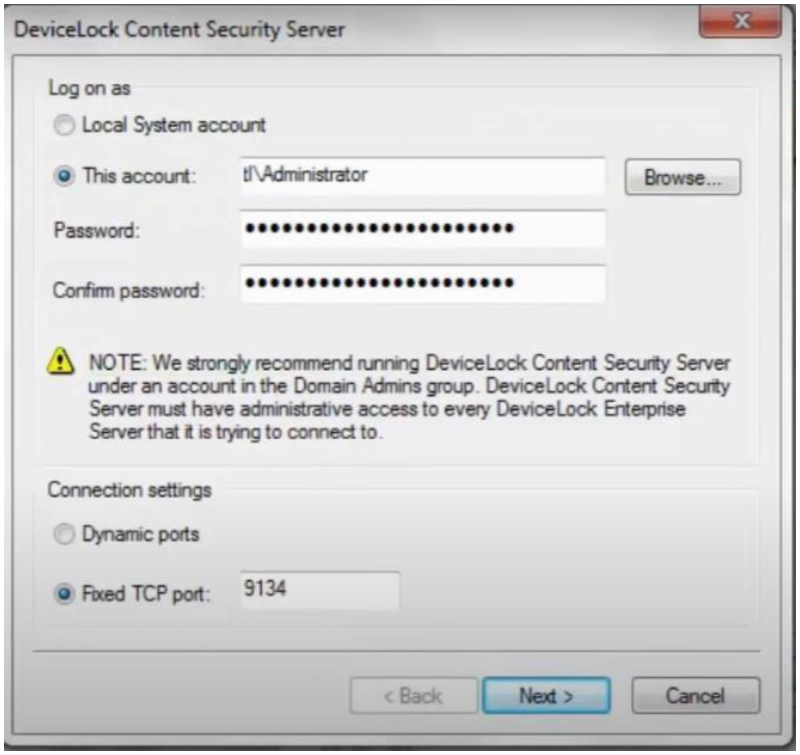

Рисунок 3.8 – Початкове налаштування DeviceLock Security Server

На наступному етапі необхідно вказати рівні доступу користувачів зареєстрованих в системі та права доступу до сервера (рисунок 3.9).

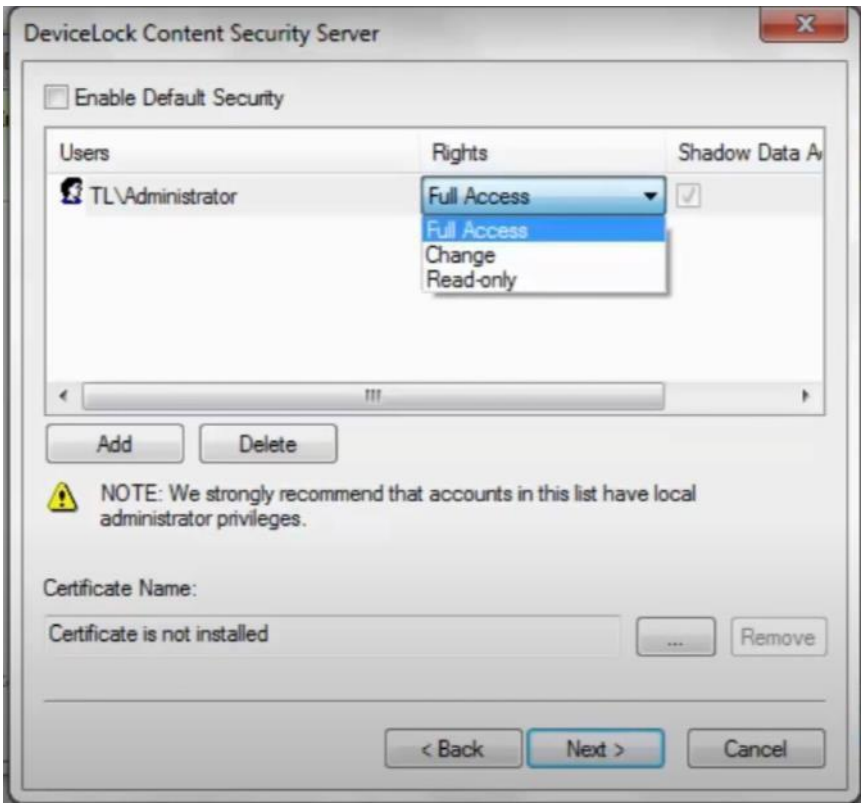

Рисунок 3.9 – Встановлення прав доступу до DLP сервера

Необхідно встановити обліковий запис для запуску служби DeviceLock Content Security Server. Це може бути локальний обліковий запис системи або інший обліковий запис.

На завершальному етапі буде відображена ліцензія на програмне забезпечення (рисунок 3.10).

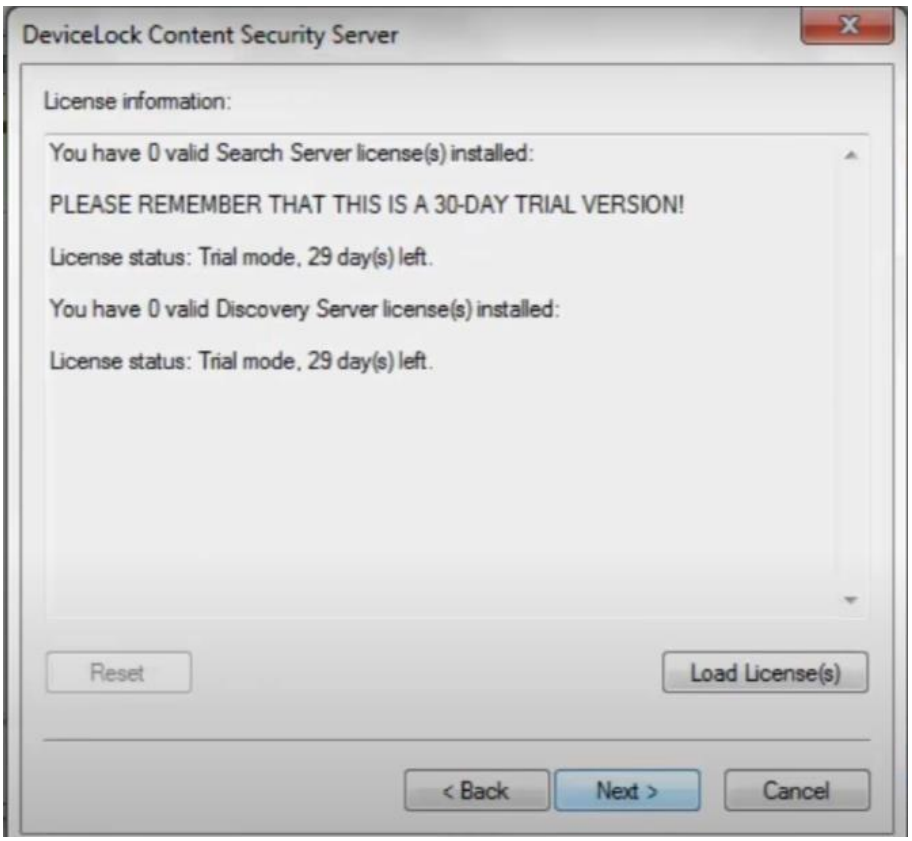

Рисунок 3.10 – Інформація про ліцензію DeviceLock Security Server

Після виведення інформації про ліцензію адміністратору потрібно буде ввести інформацію для підключення до сервера бази даних SQL. Необхідно внести назву бази-даних (БД), тип підключення, назву сервера та параметри автентифікації. Підключення до БД наведено на рисунку 3.10.

Створення бази даних займе деякий час. Якщо база даних вже існує на вказаному сервері і має правильний формат (створена програмою налаштування DeviceLock), то DeviceLock Enterprise Server використовуватиме існуючу БД.

При підключенні до мережі інтернет та при наявності ліцензії DeviceLock автоматично оновлює базу даних до останньої версії.

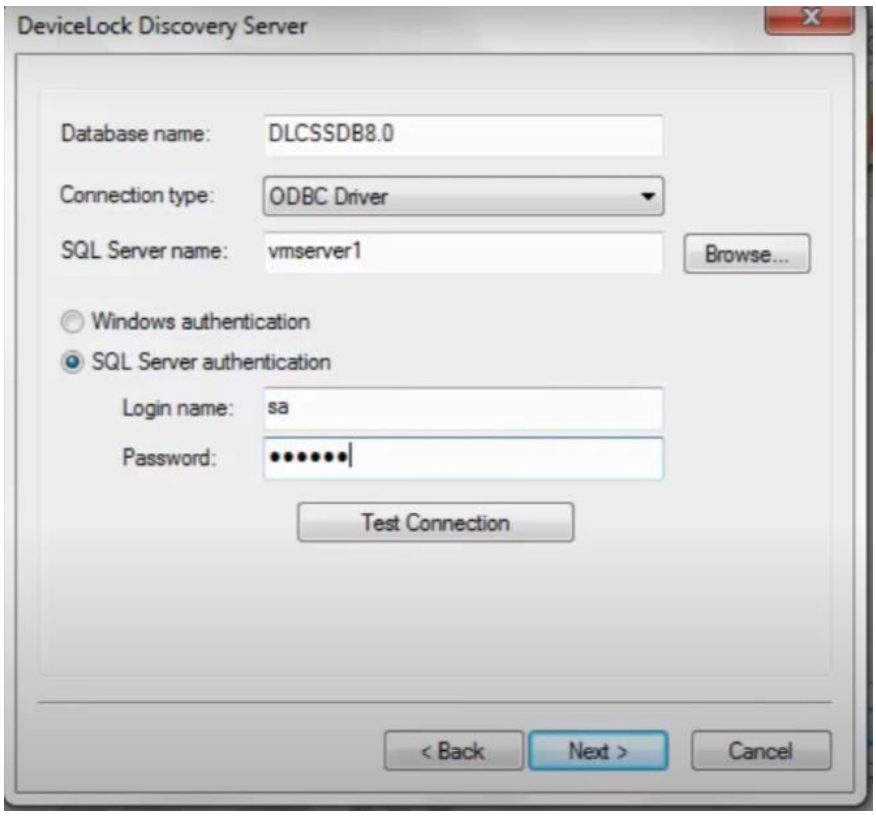

Рисунок 3.11 – Параметри підключення до БД

DeviceLock Content Security Server можна настроїти на використання певного TCPпорту для зв'язку з консоллю управління: виберіть опцію Фіксований TCP-порт та введіть номер порту. Для автоматичного вибору порту виберіть опцію Динамічна прив'язка портів. За замовчуванням DeviceLock Content Security Server використовує порт 9134.

Якщо користувач, який запустив майстер налаштування, не є адміністратором DeviceLock

Content Security Server (у ситуації, коли встановлюється оновлення поверх вже настроєного сервера), майстер налаштування не зможе встановити службу сервера і внести зміни до його параметрів. З'явиться таке повідомлення: “Доступ заборонено”. Та ж помилка може виникнути, якщо цей користувач не має права адміністратора на комп'ютері, де виконується установка DeviceLock Content Security Server.

Консолі служать для дистанційного керування сервісом DeviceLock, сервером DeviceLock Enterprise Server та сервером DeviceLock Content Security Server.

Консолі управління встановлюють на комп'ютері, з якого керуватимуться сервіс DeviceLock та сервери DeviceLock, встановлені на інших комп'ютерах. При цьому не потрібно встановлювати консолі управління на будь-який сервер (наприклад, контролер домену). Навіть якщо планується використовувати DeviceLock Group Policy Manager для управління налаштуваннями DeviceLock через групові політики Active Directory, адміністратор може робити це зі свого робочого комп'ютера (за наявності необхідних прав доступу до домену Active Directory). Вибір компонентів встановлюваного продукту ілюструє рисунок 3.12.

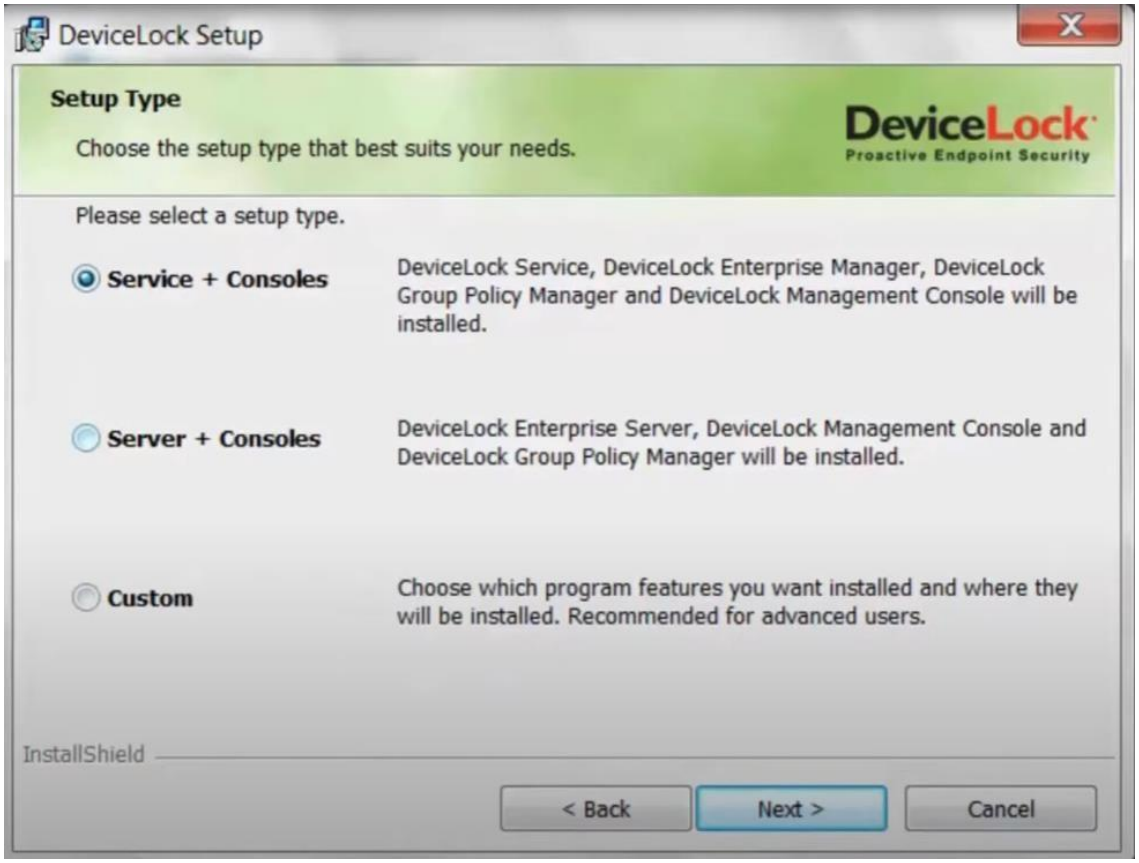

Рисунок 3.12 – Вибір компонентів встановлюваного продукту

Встановити DLP сервіс можна за допомогою декількох шляхів. Використовуючи пакет встановлення або ж використовувати команди консолі (рисунок 3.13).

Для встановлення консолей управління необхідно обрати вибіркову інсталяцію або ж вони будуть встановлені разом з компонентами сервера чи клієнтської машини.

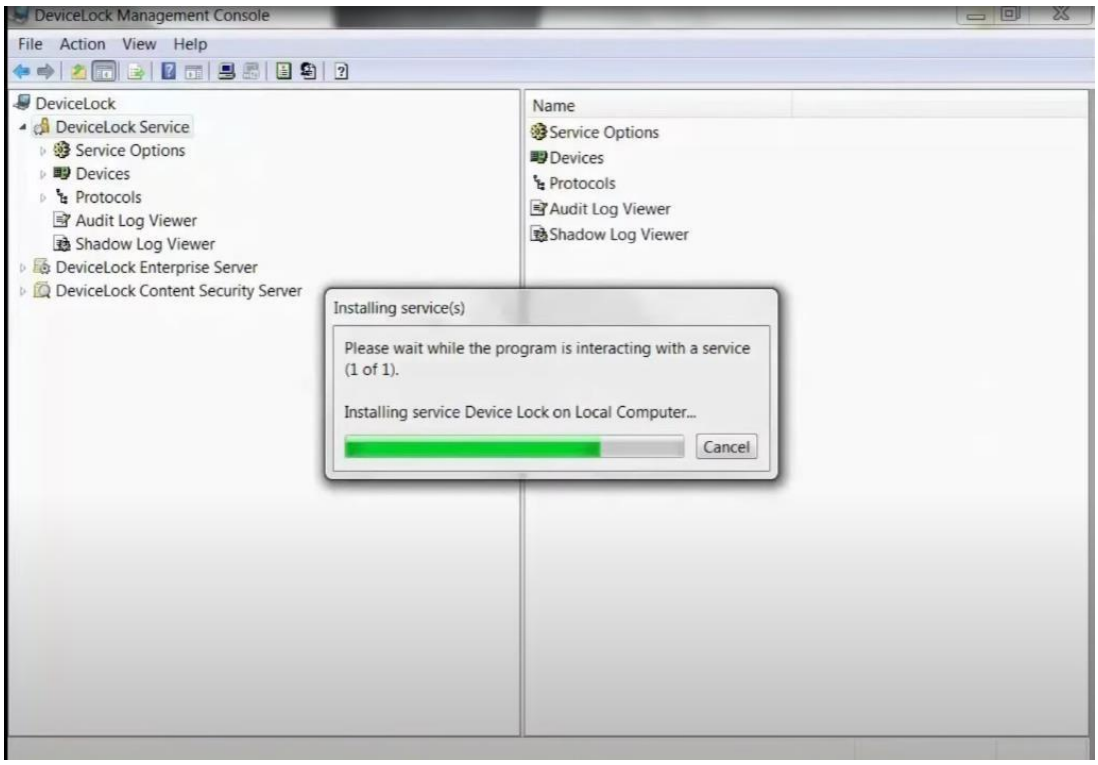

Рисунок 3.13 – Встановлення DLP сервісу через консоль керування

При встановленні через мережевий менеджер необхідно обрати плагін для встановлення, як показано на рисунку 3.14.

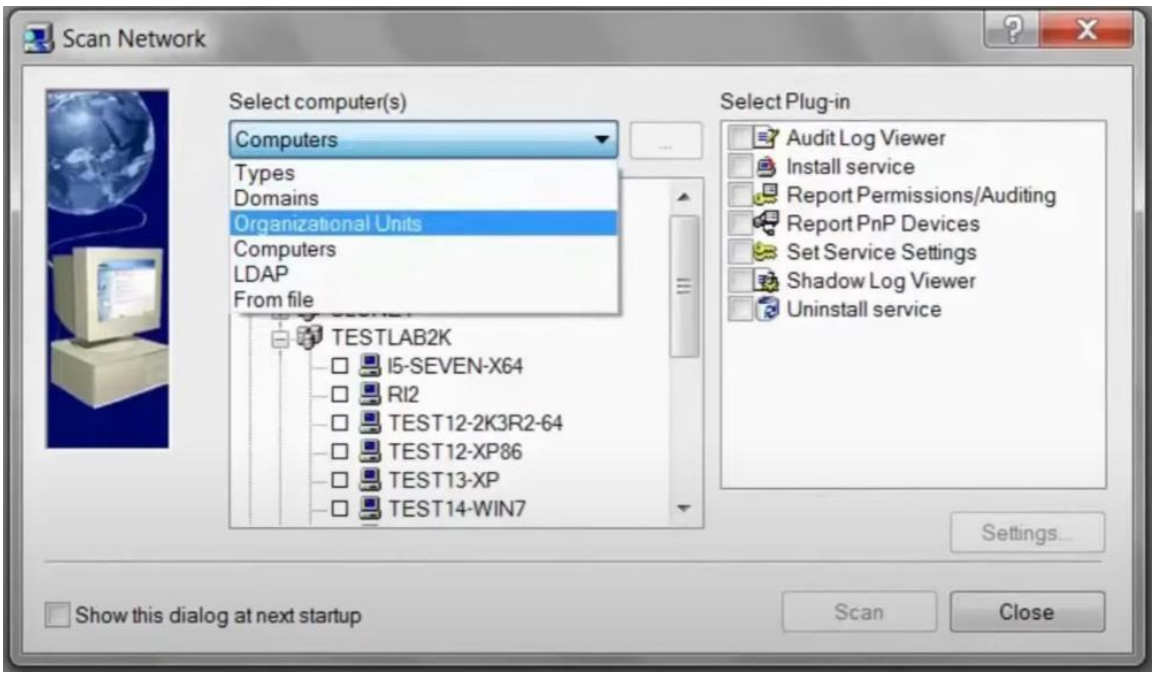

Рисунок 3.14 – Встановлення DLP сервісу використовуючи мережевий менеджер

Консолі управління встановлюють на комп'ютері, з якого керуватиме сервісом DeviceLock та сервери DeviceLock, встановлені на інших комп'ютерах. При цьому не потрібно встановлювати консолі управління на будь-який сервер (наприклад, контролер домену). Навіть якщо планується використовувати DeviceLock Group Policy Manager для управління налаштуваннями DeviceLock через групові політики Active Directory, адміністратор може робити це зі свого робочого комп'ютера (за наявності необхідних прав доступу до домену Active Directory).

3.4. Висновки до розділу

1) Серед сучасних DLP систем DeviceLock характеризується високою ефективністю та відносно низькими системними вимогами. Інтеграція DLP системи в windows дозволяє без проблем використовувати продукти Microsoft.

2) DeviceLock Group Policy Manager інтегрується у редактор управління груповими політиками Windows і недоступний як окрема програма. Для нього використання потрібно відкрити об'єкт групової політики у цьому редакторі.

3) Було проаналізовано процес та можливі сценарії встановлення DeviceLock DLP для операційної системи Microsoft.

4) Проаналізовано алгоритми контролю доступу до пристроїв та сервісів на клієнтських комп’ютерах.

4. Експериментальна перевірка

4.1. Налаштування агента DeviceLock DLP

Налаштування агентів DeviceLock DLP можна виконувати в кожній з доступних консолей. Налаштуємо DeviceLock Management Console. Це пов'язано з тим, що можливості DeviceLock Enterprise Manager та DeviceLock Group Policy Manager призначені для управління агентами в корпоративному середовищі на великій кількості робочих станцій, тоді як DeviceLock Management Console призначена для управління серверами та окремими агентами системи (рисунок 4.1).

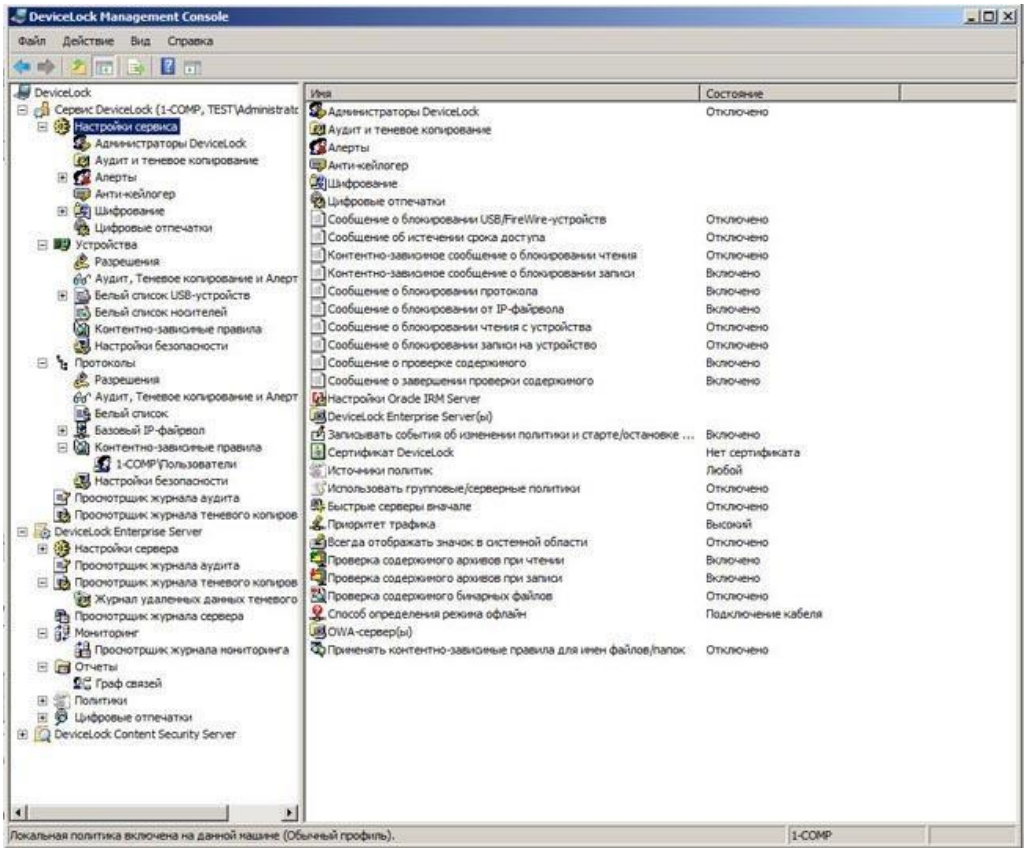

Рисунок 4.1 - Налаштування сервісу в консолі DeviceLock Management Console

Крім цього, DeviceLock Management Console є універсальним інструментом за рахунок можливості вбудовування у звичну адміністраторів

MMC-консоль. При підключенні до консолі DeviceLock DLP адміністратору безпеки надається можливість настроїти велику кількість параметрів, таких як облікові записи адміністраторів, параметри шифрування, аудиту, тіньового копіювання та оповіщення адміністратора у разі реєстрації події.

Захист від несанкціонованого доступу (рисунок 4.2) у DeviceLock DLP реалізовано функцію anti-tamper, або захист від несанкціонованого доступу — здійснюється заборона на підключення до агента DeviceLock Service, його зупинення та видалення від імені користувача, який не має на це привілеїв (навіть для локального адміністратора робочої станції).

У налаштуваннях системи можна вказати перелік облікових записів, які можуть отримати доступ до сервісу DeviceLock, зупиняти або видаляти його, а також рівень доступу - повний доступ, зміна тільки читання.

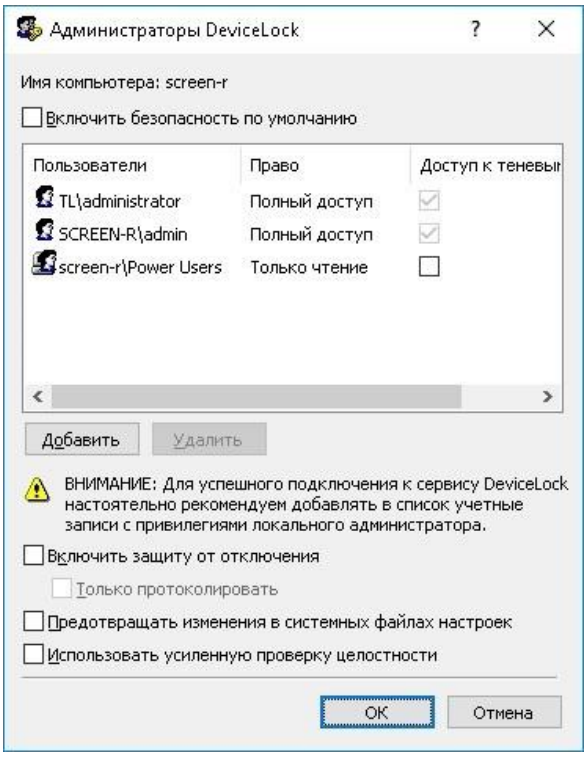

Рисунок 4.2 - Захист від несанкціонованого доступу

Також у DeviceLock можна включити захист від відключення, який активує додатковий захист проти програм для виявлення та видалення руткітів. Такі програми можуть бути використані для відключення сервісу

системи. При порушенні цілісності коду буде викликана критична помилка (наприклад, BSOD для Windows).

4.2. Контроль месенджерів

У DeviceLock DLP можна гнучко обмежити можливості використання месенджерів, які будуть доступні співробітнику: від повної заборони на роботу як через програму, так і через веб-браузер (наприклад, для WhatsApp та Telegram) до обмеження лише окремих дій. Наприклад, у програмі буде дозволено надсилання та отримання повідомлень, але заборонено надсилання вихідних файлів або дзвінків (для Skype). У той же час для однієї й тієї ж програми можна дозволити роботу лише через програму або лише через веббраузер. Крім політик дозволів, на агенті можна додати правило створення тіньових копій повідомлень і файлів, що передаються, а також налаштувати відправлення оповіщень адміністратору у випадку, коли співробітник використовує програму. Для всіх програм можна настроїти дозволений та заборонений час використання. Якщо встановлено заборону на запуск, система виведе налаштовуване повідомлення про відсутність прав доступу до месенджера (рисунок 4.3).

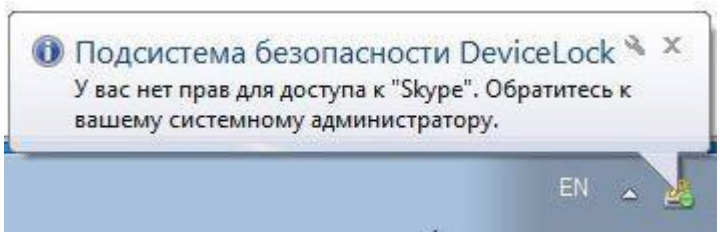

Рисунок 4.3 - Заборона використання Skype на робочому місці

Для контролю Skype існують унікальні налаштування, які дозволяють дозволити або заборонити надсилання та отримання даних, вхідні та вихідні дзвінки та повідомлення. Окремо можна встановити заборону вихідних файлів.

При забороні дзвінків співробітник зможе почати дзвінок у Skype, але як тільки співрозмовник прийме дзвінок, дзвінок обірветься, при цьому в інтерфейсі Skype буде відображено пропущений дзвінок (рисунок 4.4).

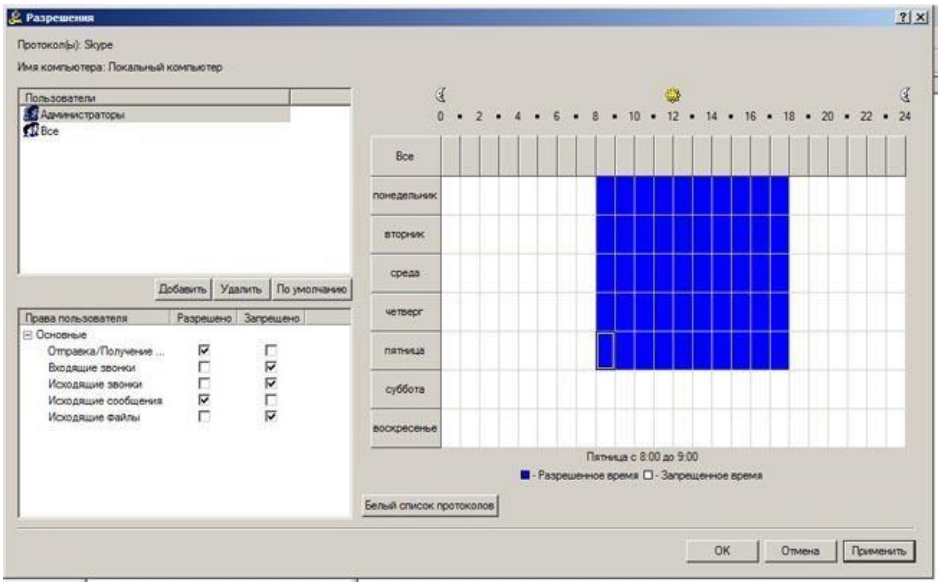

Рисунок 4.4 - Заборона здійснювати вихідні та вхідні дзвінки у Skype

Причому якщо під час дії політики, яка забороняє вихідні повідомлення, співробітник намагався їх надіслати, то після зміни політики та дозволу на зазначені дії всі повідомлення будуть доставлені адресатам.

Проведемо налаштування політики аудиту, тіньового копіювання та сповіщень для Skype у DeviceLock DLP, як це показано на рисунку 4.5.

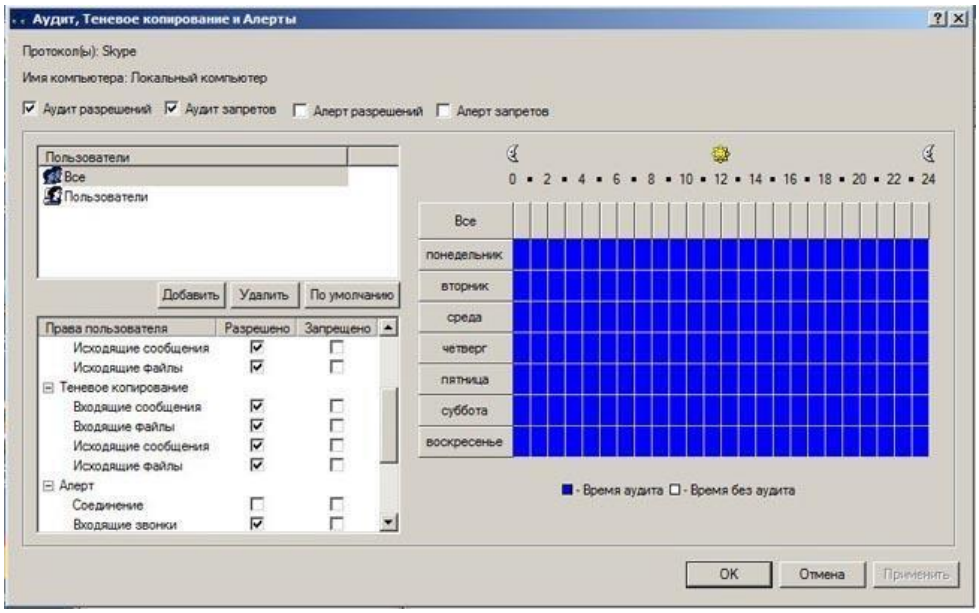

Рисунок 4.5 - Налаштування DeviceLock DLP

Існує можливість вибору груп користувачів та проведення аудиту заборон. Також функціонал DLP дозволяє тонке налаштування реагування на інциденьт правил безпеки.

Проведемо тестування виконання інциденту по протоколу Skype, спробувавши надіслати файл (рисунок 4.6).

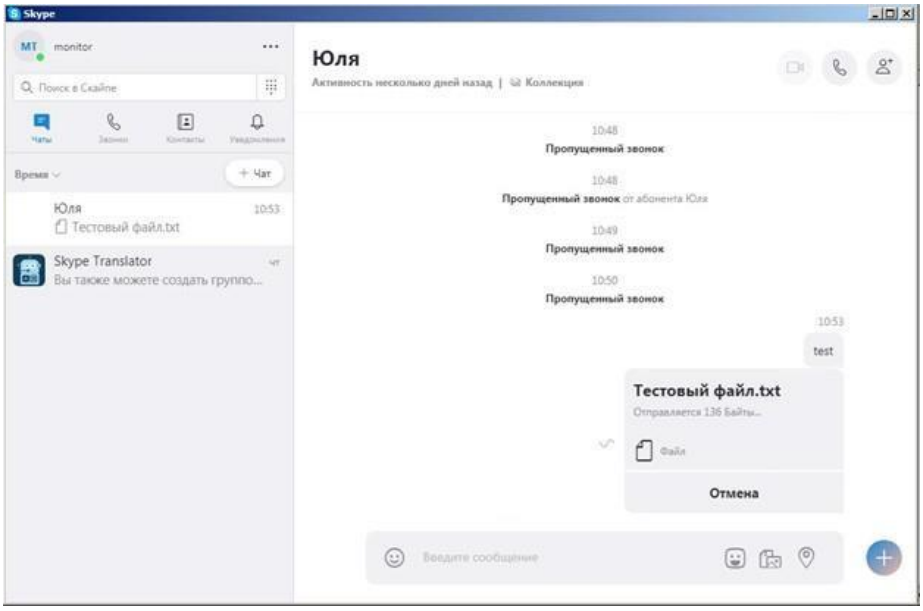

Рисунок 4.6 - Skype очікує дозволу надсилання вихідного файлу

Контроль WhatsApp Для контролю за програмою WhatsApp у DeviceLock DLP настройок менше — можна задати час дозволеного використання програми або повністю заборонити відправлення та отримання даних. При цьому працівник не зможе пройти процедуру автентифікації у додатку. Проте, якщо працівник запустить програму у дозволений час, то зможе продовжити комунікацію і після заборони (рисунок 4.7).

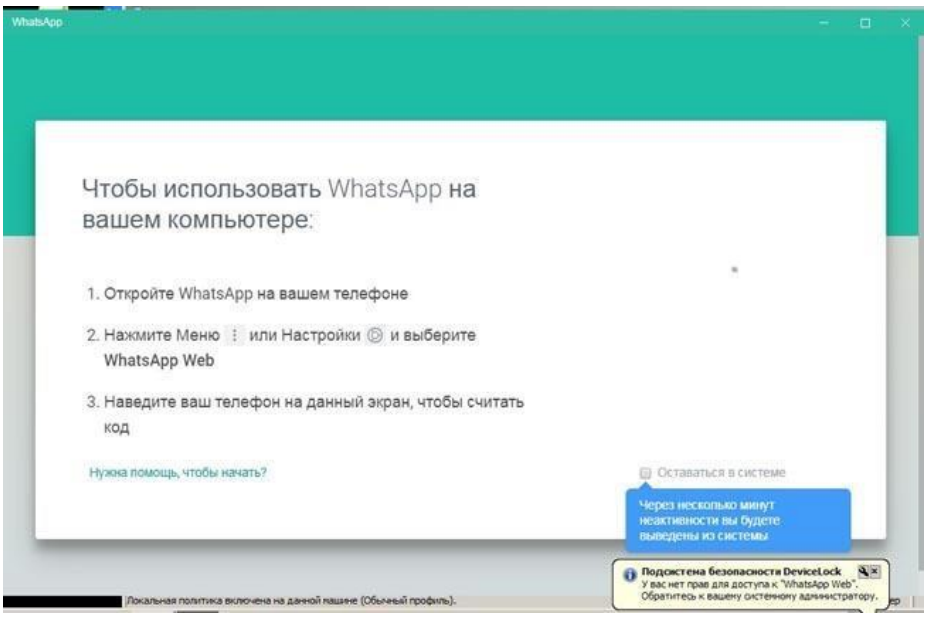

Рисунок 4.7 - При забороні роботи в WhatsApp співробітник не зможе автентифікуватись у додатку

Контроль Telegram За допомогою DeviceLock DLP можна заборонити запуск програми Telegram, а також роботу з ним через офіційний веб-сайт.

При роботі з Telegram необхідно врахувати можливість доступу до ресурсу через веб-інтерфейс. Для цього потрібно створити правило для реагування на інциденти, як це показано на рисунку 4.8.

При роботі з веб протоколом є можливість лише заборонити чи дозволити відправку або отримання даних.

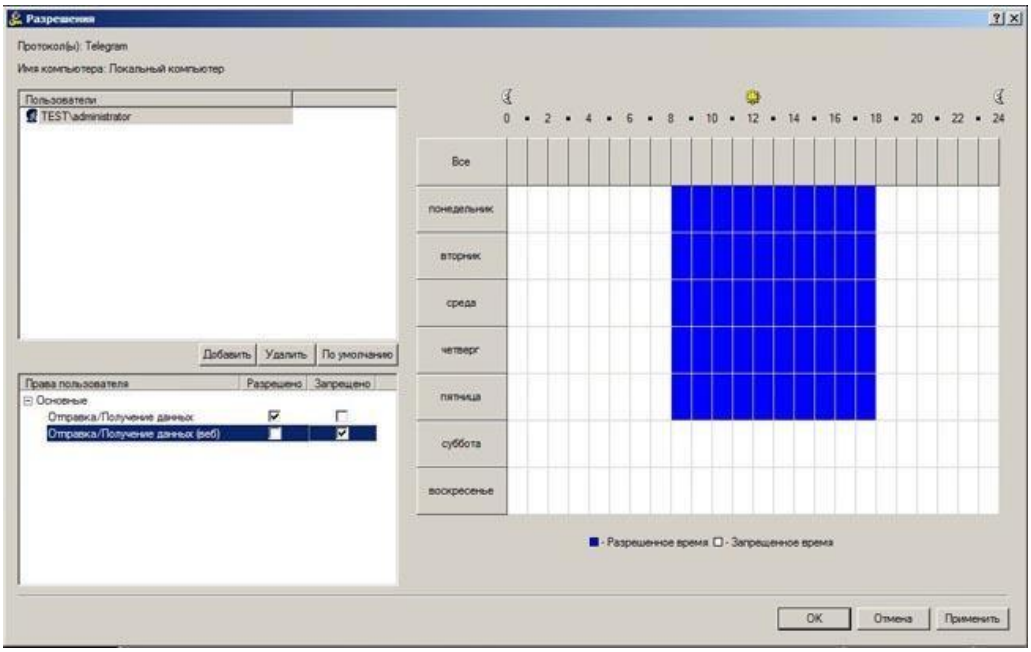

Рисунок 4.8 - Дозволи та заборони окремо для програми Telegram та доступу до нього через веб-браузер

Тестування показало, що система працює ефективно і виконуються дії, як і було заплановано.

4.3. Контроль хмарних сервісів

Політики контролю хмарних сервісів можуть дозволяти відправлення та отримання даних, так і забороняти мережевий обмін файлами. Після налаштування забороняючих DLP-політик щодо роботи з хмарними сервісами у співробітника пропаде можливість роботи з хмарою.

Наприклад, GoogleDisk видасть помилку вже на етапі встановлення програми («Не вдалося завантажити»), Google Drive не зможе увійти до облікового запису. Для блокування роботи з Google Drive заблокуємо SSL Post запити, як це показано на рисунку 4.9.

Приклад блокування роботи з Google Drive приведени на рисунку 4.10.

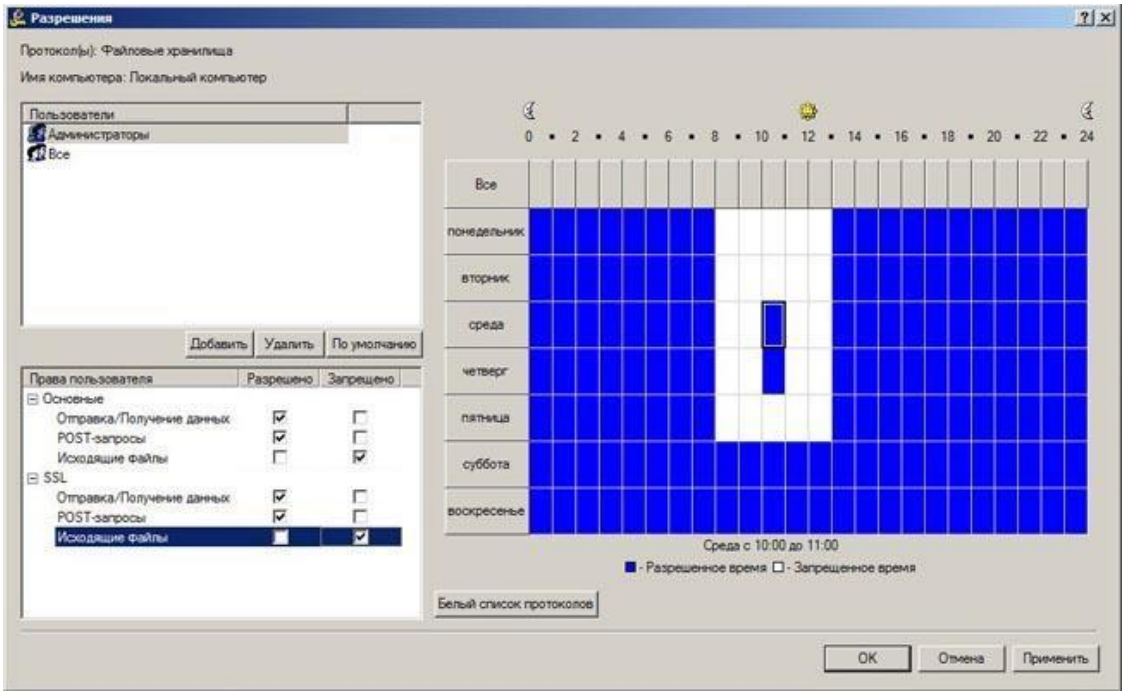

Рисунок 4.9 - У DeviceLock DLP можна заборонити лише надсилання документів у хмару, дозволивши інші дії з файлами

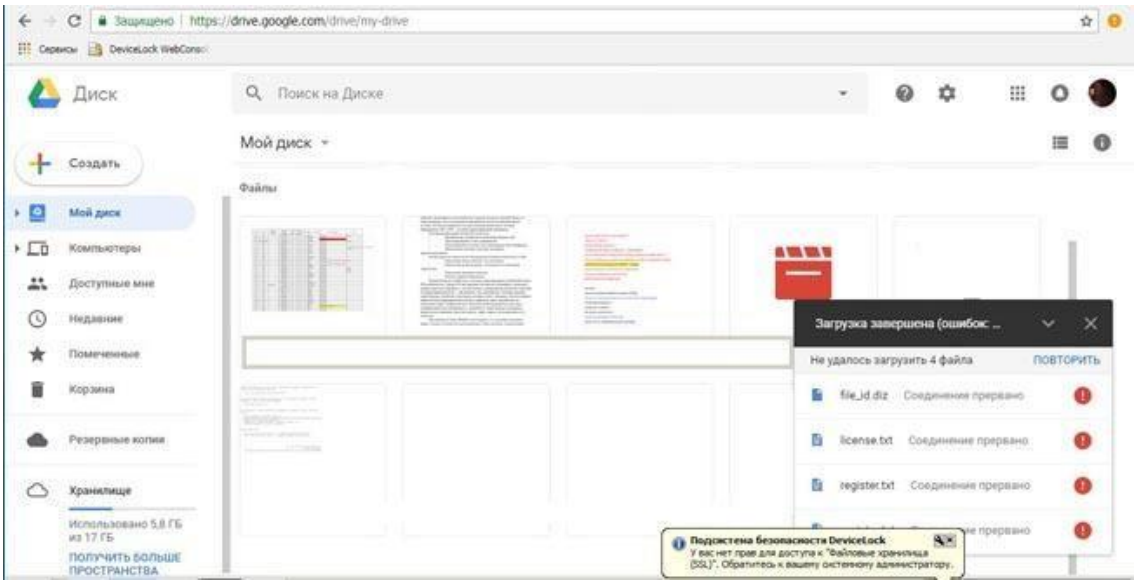

Рисунок 4.10 - Спроба завантажити файл у Google Drive

При цьому якщо програми вже були встановлені, то можливість роботи із синхронізованими файлами залишиться, але буде заборонено завантаження документів у хмару. Крім зазначених програм, у новій версії DeviceLock DLP додано можливість контролю роботи з сервісами файлового обміну та синхронізації iCloud та WeTransfer та 4shared, Box.com, GMX.de та Web.de. Що стосується доступу через веб-браузер, в налаштуваннях агента можна встановити дозвіл та заборони на надсилання/отримання даних, POST-запити та вихідні файли.

4.4. Контроль трафіку браузера Tor

Щоб заборонити працівникам роботу через браузер Tor, у новій версії DeviceLock DLP з'явилася можливість заблокувати трафік браузера. У налаштуваннях безпеки агента DeviceLock можна заборонити інші типи передачі трафіку, такі як непізнаний вихідний SSL-трафік, проксі-трафік, з'єднання MS Lync та інші (рисунок 4.11).

Рисунок 4.11 - DeviceLock DLP забороняє браузеру Tor встановлювати захищене з'єднання

Контроль трафіку BitTorrent DeviceLock DLP має окрему політику, яка дозволяє заборонити відправлення та отримання даних за протоколом BitTorrent. При ввімкненні цієї політики на екрані з'явиться повідомлення про заборону використання програми, але сама програма відкриється, хоча так і не зможе підключитися до бенкетів для прийому файлу (рисунок 4.12).

Рисунок 4.12 - DeviceLock DLP може блокувати трафік у торент-клієнтах

Контроль зовнішніх пристроїв У правилах контролю доступу до пристроїв можна гнучко налаштувати розклад дії правила, вказати облікові

записи працівників, на які поширюється правило, та дії, які можна або заборонено виконувати з файлами (включаючи їх створення) на пристроях. Для тесту створимо необхідне правило для USB порта. Вкажемо флаги доступу та часові обмеження. Це правило буде спрацьовувати з обраними користувачами надаючи чи забороняючи їм доступ до носія, як це показано на рисунку 4.13.

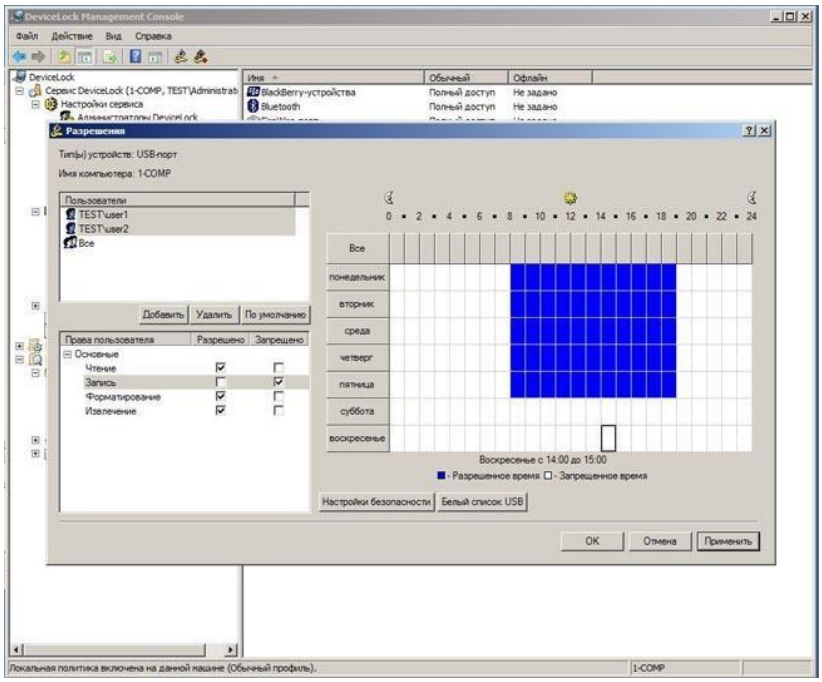

Рисунок 4.13 - Налаштування дозволів використання USB-пристроїв у DeviceLock Management Console

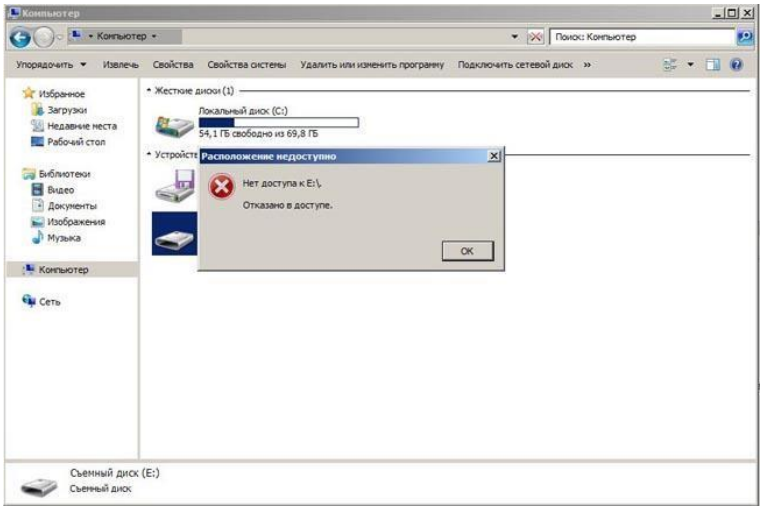

Рисунок 4.14. Заборона доступу до знімного носія відповідно до політики дозволів

Налаштування правил контентної фільтрації у версії DeviceLock DLP 8.3 були додані нові словники для контентної фільтрації та шаблони регулярних виразів, які дозволяють адміністратору безпеки гнучко настроїти правила виявлення несанкціонованої передачі конфіденційних даних, що може призвести до їх витоку.

У DeviceLock з'явився новий спосіб контентної фільтрації - використання цифрових відбитків файлів, які дозволяють ідентифікувати дані за рахунок порівняння з хешами документів (рисунок 4.15).

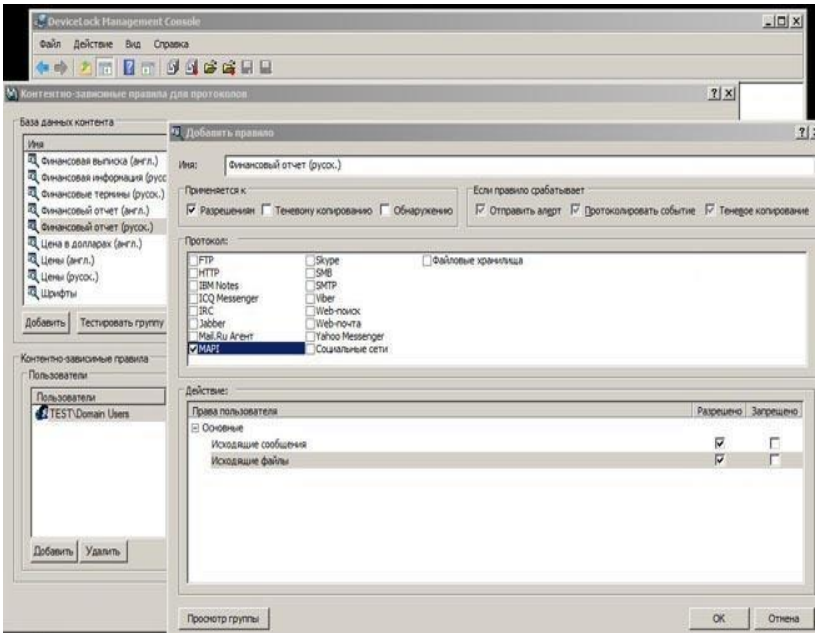

Рисунок 4.15 - У DeviceLock DLP можна налаштувати різні правила контентнозалежних правил для груп користувачів

Налаштування надсилання повідомлень по SYSLOG DeviceLock DLP має можливість надсилання даних за протоколом SYSLOG, наприклад, для інтеграції з існуючою системою SIEM.

У налаштуваннях агента можна задати типи повідомлень та перевірити їхнє надсилання (рисунок 4.16).

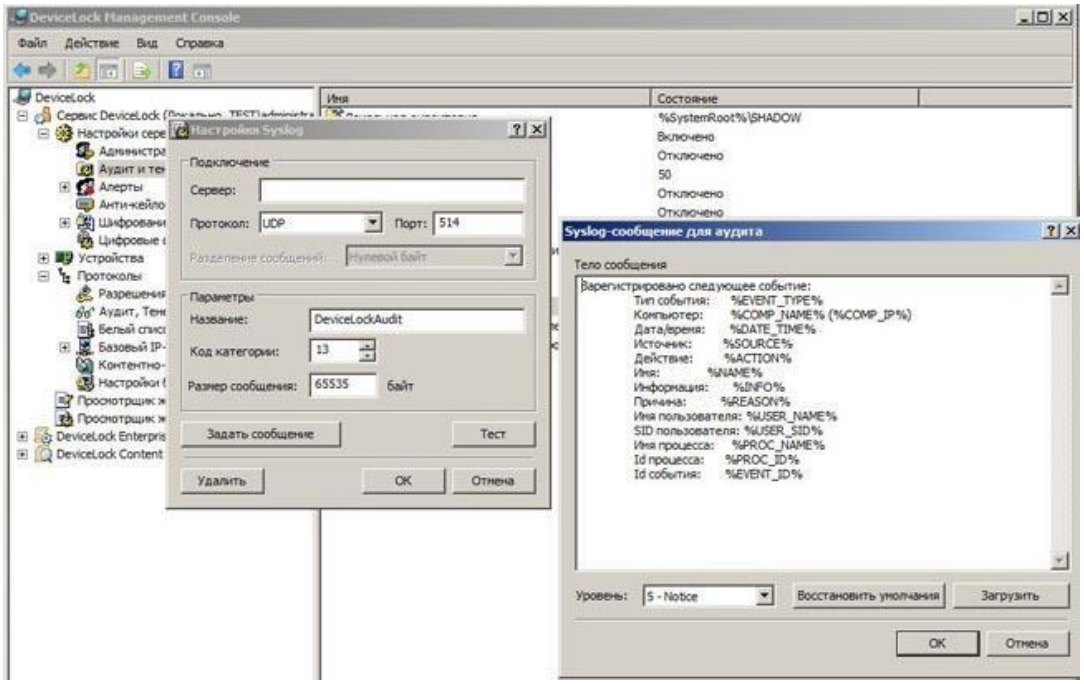

Рисунок 4.16 - Можливості DeviceLock DLP дозволяють швидко налаштувати інтеграцію до SIEM-системи

Цей метод може ефективно застосовуватися, наприклад, для типових текстових документів, креслень, графічних та бінарних файлів.

4.5. Висновки до розділу

1) DeviceLock DLP можна віднести до типу хостових DLP, в яких не потрібна можливість зняття трафіку з проксі-сервера, SPAN-порту та інших периметральних пристроїв.

2) До переваг DeviceLock можна выднести можливість контролю дистанційних працівників, які не знаходяться в офісі, за рахунок архітектури хостової DLP-системи (автономне функціонування агента DLP-системи). Можливість вибіркового запобігання витоку в реальному часі для закритих пропрієтарним шифруванням мережевих сервісів, у тому числі на підставі аналізу вмісту даних, що передаються.

3) До недоліків DeviceLock можна віднести відсутність підтримки операційних систем Linux та відсутність функцій поведінкового аналізу користувачів (UBA).

ВИСНОВКИ

Розглянуто та дано визначення основних понять та термінів, які використовуються системах захисту інформації, що дозволило визначити основні види запобігання витоку інформації.

Проаналізовано актуальність використання DLP-систем для забезпечення належного стану інформаційної безпеки та розслідування інцидентів.

Сформульовано завдання на проектування системи управління інцидентами інформаційної безпеки на основі DLP-систем, яке включає вхідні та вихідні дані та можливі обмеження.

Проаналізовано методи ідентифікації і аналізу даних в DLP-системах та обрано систему, що характеризується оптимальними характеристиками та функціональністю для реалізації даної дипломної роботи.

Запропоновано алгоритм захисту від несанкціонованого доступу до інформації, що дозволяє підвищити стійкість обраної DLP системи.

Виконано встановлення DLP DeviceLock та проаналізовано можливі варіанти налаштування сервісу. Серед сучасних DLP систем DeviceLock характеризується високою ефективністю та відносно низькими системними вимогами. Інтеграція DLP системи в windows дозволяє без проблем використовувати продукти Microsoft.

Проаналізовано алгоритми контролю доступу до пристроїв та сервісів на клієнтських комп’ютерах та архітектура DLP системи та виконано налаштування на комп’ютерах з ОС Windows.

Проведено аналіз переваг DeviceLock до яких можна віднести можливість контролю дистанційних працівників, які не знаходяться в офісі, вибіркового запобігання витоку в реальному часі для закритих пропрієтарним

шифруванням мережевих сервісів, у тому числі на підставі аналізу вмісту даних, що передаються. До недоліків DeviceLock можна віднести відсутність підтримки операційних систем Linux та відсутність функцій поведінкового аналізу користувачів (UBA).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник.- Київ: ООО Д.В.К., 2004. - 508 с.

2. Шумейко О.О. Інформаційна безпека.- Дніпровський державний технічний університет, 2019. — 155 с.

3. Антонюк А.О. Теоретичні основи захисту інформації.- Київ: НТУУ "КПІ", 2003. — 233 с.

4. Donaldson S.E., Siegel S.G., Williams C.K., Aslam A. Enterprise Cybersecurity.- Apress, 2015. — 536 p.

5. Brooks C. et al. Cybersecurity Essentials.- Sybex, 2018. — 768 p.

6. Bermudez Marlon. Cybersecurity for Small and Midsize Businesses.- BookBaby, 2020. — 224 p.

7. Santos O. Developing Cybersecurity Programs and Policies.- Pearson IT Certification, 2018. — 672 p

8. Ackerman Pascal. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment.- 2nd edition. — Packt Publishing, 2021. — 800 p.

9. Thompson E.C. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents.- Apress, 2018. — 184 p.

10. Широчин В.П., Широчин С.В., Мухін В.Є. Основи безпеки комп'ютерних систем.- Навч. посібник. - К.: "Корнійчук", 2009. - 286 с.

11. Бурячок В.Л. та ін. Інформаційна та кібербезпека: соціотехнічний аспект.- Підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. — Київ: ДУТ, 2015. — 288 с.

12. Ahmad Khaleel et al. Emerging Security Algorithms and Techniques.- Khaleel Ahmad, M.N. Doja, Nur Izura Udzir, Manu Pratap Singh. — CRC Press, 2019. — 331 p.

13. Офіційний сайт Міжнародного фонду збору інформації про комп'ютерні інциденти в світі DataLossDB [Електронний ресурс]. – Режим доступу: http://Datalossdb.org/statistics

14. Що робити компанії в разі витоку інформації? [Електронний ресурс].- Режим доступу: https://uteka.ua/publication/news-14-delovye-novosti-36-shhorobiti-kompanii-v-razi-vitoku-informacii

15. DLP-система Solar [Електронний ресурс].- Режим доступу: https://servernews.ru/978630

16. Территориально распределенная безопасность: как сделать, чтобы реально работало [Електронний ресурс].- Режим доступу: https:// www.securitylab.ru/analytics/531185.php

17. Forcepoint DLP [Електронний ресурс].- Режим доступу: https://roi4cio.com/catalog/product/forcepoint-dlp

18. Forcepoint DLP - система защиты от утечек даннях [Електронний ресурс].- Режим доступу: https://msmax.kz/endpoint

19. Symante Data Loss Prevention [Електронний ресурс].- Режим доступу: ttps://static.carahsoft.com/concrete/files/9814/4734/5158/ Data_Loss_ Prevention_Data_Insight_Enterprise.pdf

20. Symantec Data Loss Prevention Solution [Електронний ресурс].- Режим доступу: https://docs.broadcom.com/doc/data-loss-prevention-solution-en

21. Офіційний сайт McAfee DLP [Електронний ресурс].- Режим доступу: https://www.mcafee.com

22. McAfee Data Loss Prevention Endpoint [Електронний ресурс].- Режим доступу: https://softlist.com.ua/catalog/product-mcafee-dlp/

23. Офіційний сайт Sophos [Електронний ресурс].- Режим доступу: https://www.sophos.com

24. Sophos Endpoint Protection [Електронний ресурс].- Режим доступу: https://spro.com.ua/products/sophos/sophos-endpoint-protection

25. An enterprise DLP that’s easy to learn, deploy, and manage [Електронний ресурс].- Режим доступу: https://www.acronis.com/en-us/products/devicelock 26. Посібник користувача [Електронний ресурс].- Режим доступу: https://dl.acronis.com/u/pdf/Acronis-DeviceLock-DLP-9.0-Man_ru-RU.pdf