Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїі*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Аналіз програмних засобів запобігання витоку інформації

(тема)

Виконав:
студент 2 курсу, групи *ІМІм-20-2*
Пестєрєва С.Є.

Спеціальності *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц., к.т.н. Чеботарьова Д.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2022 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Пестєрєва С.Є.*
(підпис) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри ІМІ_____
(підпис)
“____” _____2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентові *Пестєрєвій Софії Євгенівні*
(прізвище, ім’я, по батькові)

1. Тема роботи *Аналіз програмних засобів запобігання витоку інформації*

затверджені наказом університету від *14 березня 2022* року № *379 Ст*

2. Термін подання студентом роботи до екзаменаційної комісії *13 травня 2022 р.*

3. Вихідні дані до роботи

Дослідити технології запобігання витоку інформації, зокрема: системи виявлення та запобігання вторгнень, антивірусне програмне забезпечення, системи управління інформацією та подіями безпеки, DLP-системи та брандмауери. Проаналізувати основні характеристики DLP-систем та особливості роботи цих систем з інформацією, що перебуває у різних станах. Дослідити сучасні програмні засоби запобігання витоку інформації та виконати порівняльний аналіз цих програмних продуктів.

4. Перелік питань, що потрібно опрацювати в роботі

Вступ
1. Технології запобігання витоку інформації
2. Основні характеристики DLP-систем
3. Аналіз станів DLP-системи
4. Програмні засоби запобігання витоку інформації
5. Аналіз програмних засобів запобігання витоку інформації
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *Слайди у форматі Power Point (назва, мета і задачі роботи, основні причини для запобігання втат даних, технології захисту інформації, основні функції DLP-систем, переваги та недоліки DLP-систем, три основні інформаційні стани інформації, програмні засоби запобігання витоку інформації, порівняння програмного забезпечення DPL, аналіз програмних засобів запобігання витоку інформації, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ*	*14.03.22*	*виконано*
2	*Підбір літератури за темою роботи*	*15.03-18.03.22*	*виконано*
3	*Виконання розділу 1*	*19.03-29.03.22*	*виконано*
4	*Виконання розділу 2*	*30.03-09.04.22*	*виконано*
5	*Виконання розділу 3*	*10.04-20.04.22*	*виконано*
6	*Виконання розділу 4*	*21.04-01.05.22*	*виконано*
7	*Виконання розділу 5*	*02.05-08.05.22*	*виконано*
8	*Оформлення пояснювальної записки*	*09.05-11.05.22*	*виконано*
9	*Оформлення презентаційного матеріалу,*	*12.05-13.05.22*	*виконано*
	підготовка до захисту у ЕК		

Дата видачі завдання *14.03.2022 р.*

Студент _____ *Пестєрєва С.Є.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 с., 23 рис., 2 табл., 18 джерел, 2 додатки.

Об'єкт дослідження – програмні засоби запобігання витоку інформації.

Мета роботи – порівняльний аналіз програмних засобів запобігання витоку інформації.

Результати – в роботі досліджено технології запобігання витоку інформації, а саме: системи виявлення та запобігання вторгнень, антивірусне програмне забезпечення, системи управління інформацією та подіями безпеки, DLP-системи та брандмауери. Проаналізовано основні характеристики DLP-систем та особливості роботи цих систем з інформацією, що перебуває у різних станах. Досліджено сучасні програмні засоби запобігання витоку інформації та виконано порівняльний аналіз цих програмних продуктів.

DLP, ІНФОРМАЦІЯ, ЗАХИСТ, БЕЗПЕКА, ДАНІ, ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ, КОМПАНІЯ, ПРОГРАМНИЙ ЗАСІБ, СТАН

THE ABSTRACT

Explanatory note: 66 p., 23 fig., 2 tabl., 18 sources, 2 app.

The object of study is data loss prevention software tools.

The purpose of the work is to study comparative analysis of data loss prevention software tools.

Results – the technologies for data loss prevention have been investigated in the work, namely: intrusion detection and prevention systems, antivirus software, security information and event management, DLP-systems and firewalls. The main characteristics of DLP-systems and features of these systems with information have been analyzed, which are in different states. Modern data loss prevention software have been investigated and comparative analysis of these program product have been done.

DLP, INFORMATION, PROTECTION, SECURITY, DATA, DATA LOSS PREVENTION, COMPANY, SOFTWARE, STATUS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

BYOD (Bring Your Own Device) – IT-політика «принесіть власний пристрій»;

DLP (Data Leakage (Loss) Prevention) – технології запобігання витоку конфіденційної інформації;

HIDS (Host-Based Intrusion Detection System) – хостова система виявлення вторгнень;

HIPS (Host-based Intrusion Prevention System) – хостова система попередження вторгнень;

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертексту;

HTTPS (Hyper Text Transfer Protocol Secure A) – розширення протоколу HTTP;

IDS (Intrusion Detection Systems) – система виявлення вторгнень;

IPS (Intrusion Prevention Systems) – система попередження вторгнень;

NIDS (Network Intrusion Detection System) – мережна система виявлення вторгнень;

NIPS (Network Intrusion Prevention System) – мережна система попередження вторгнень;

SIEM (Security information and event management) – системи управління інформацією та подіями безпеки.

ВСТУП

Конфіденційність інформації є необхідною умовою для більшості компаній, тому вище керівництво компаній, адміністратори та IT-менеджери приділяють велику увагу питанням захисту інформації. Інформація в кожній компанії є одним з найважливіших активів, тому захист цих даних має бути першочерговим.

В наш час однією з найбільш актуальних проблем у сфері інформаційної безпеки є проблема захисту від витоку конфіденційної інформації. Розвиток засобів, методів та форм автоматизації процесів обробки інформації, масовість застосування конфіденційної інформації в інформаційно-комунікаційних мережах різко підвищують уразливість інформації. Основними факторами, що сприяють підвищенню цієї вразливості, є: різке збільшення обсягів інформації, що накопичується, зберігається та обробляється в інформаційних мережах; зосередження в єдиних базах даних інформації різного призначення та різної приналежності; різке розширення кола користувачів, які мають безпосередній доступ до ресурсів обчислювальних систем та масивів даних, що знаходяться в них; ускладнення режимів функціонування технічних засобів тощо. В результаті зростає ймовірність витоку інформації, який негативно впливає на компанії та організації.

Традиційні підходи безпеки, такі як брандмауери, не можуть захистити інформацію від витоку. Витік інформації відбувається, коли конфіденційні дані навмисно чи не навмисно розкриваються неавторизованим сторонам. Витік інформації може спричинити серйозні загрози для компанії. Втрата конфіденційної інформації може серйозно вплинути на репутацію компанії, довіру клієнтів і співробітників, конкурентну перевагу і в деяких випадках призвести до закриття компанії або політичних криз, таких як витоки WikiLeaks.

Проблему витоку інформації необхідно вирішувати за допомогою спеціальних систем запобігання витоку (втрати) інформації. Системи запобігання витоку (втрати) інформації DLP (Data Leakage (Loss) Prevention) – це рішення, які захищають конфіденційну інформацію, в тому числі і від потрапляння в ненадійні руки.

Рішення DLP допомагають виявляти, відстежувати, захищати та

знижувати ризики витоку конфіденційної інформації. Ці рішення використовується для виявлення та запобігання одержання конфіденційних даних неавторизованими користувачами, а також для захисту конфіденційних даних, якими можна випадково поділитися.

Метою роботи є огляд технологій запобігання витоку інформації, дослідження особливостей і основних характеристик систем DLP, а також аналіз програмних засобів для запобігання витоку інформації. Розглянуті в роботі питання є надзвичайно актуальними під час пандемії та воєнного стану, коли в нашій країні велику кількість компаній та різних організацій переведено на онлайн-роботу, а співробітникам компаній надано віддалений доступ до інформації, в тому числі і конфіденційної. Саме тому тема кваліфікаційної роботи, що присвячена аналізу програмних засобів для запобігання витоку інформації, є актуальною.

1 ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

1.1 Актуальність технологій запобігання витоку інформації

У сучасному цифровому світі, що керується даними, втрата даних є дуже серйозною проблемою. Велика кількість даних створюється на особистому рівні, а потім ця інформація завантажується в інфокомунікаційні мережі і потрапляє до тисяч чи навіть мільйонів користувачів цих мереж. У цьому контексті запобігання втраті даних має бути першочерговим завданням для власників інформації, особливо в бізнесі. Навіть найменша помилка може перешкодити належній роботі систем і навіть вплинути на безперервність бізнесу. Простої коштують дорого, тому захист від втрати даних є надзвичайно важливою проблемою. Усі компанії повинні захищати себе від втрати даних [1].

У сучасній ситуації, коли кожен по черзі працює вдома і працює в офісі, з більшою ймовірністю трапляються порушення даних та інші ризики. Великі компанії мають більше даних для крадіжки, а невеликі компанії мають менш захищені мережі, що робить їх легкою мішенню для кіберзлочинців.

Є кілька рішень, як захистити інформацію для того чи іншого бізнесу, але технології ефективні лише в тому випадку, якщо люди, відповідальні за моніторинг та керування ними. Рішення повинні доповнювати стратегію незалежно від галузі та розміру бізнесу [2].

Основні причини для запобігання втрат даних наведено на рис. 1.1. Вони повинні розглядатися як абсолютна необхідність для запобігання втрат інформації у підприємствах будь-якого розміру.

Зростання зовнішніх загроз і атак. Організації дуже серйозно ставляться до втрати даних. Однак, оскільки викрадачі даних з кожним днем стають все більш витонченими, а багато з них все частіше знаходять нові способи доступу до мереж, компанії стикаються зі зростаючим тиском, щоб активно продовжувати пошук нових загроз.

Внутрішні загрози. Неперевірені працівники є яскравим прикладом внутрішніх загроз – осіб, які свідомо мають намір завдати шкоди компанії зсередини. Вони можуть зробити це самі або спробувати знайти допомогу стороннього для здійснення нападу.

Враховуючи той факт, що вони вже мають доступ до даних, а також можуть мати деяку конфіденційну інформацію щодо різного персоналу в компанії, атака може виявитися більш небезпечною, ніж через спробу порушення з боку організації. Це особливо важливо, якщо працівник виявляється високопоставленим керівником, оскільки він зазвичай має доступ до набагато більшого обсягу конфіденційної інформації, ніж інші співробітники.

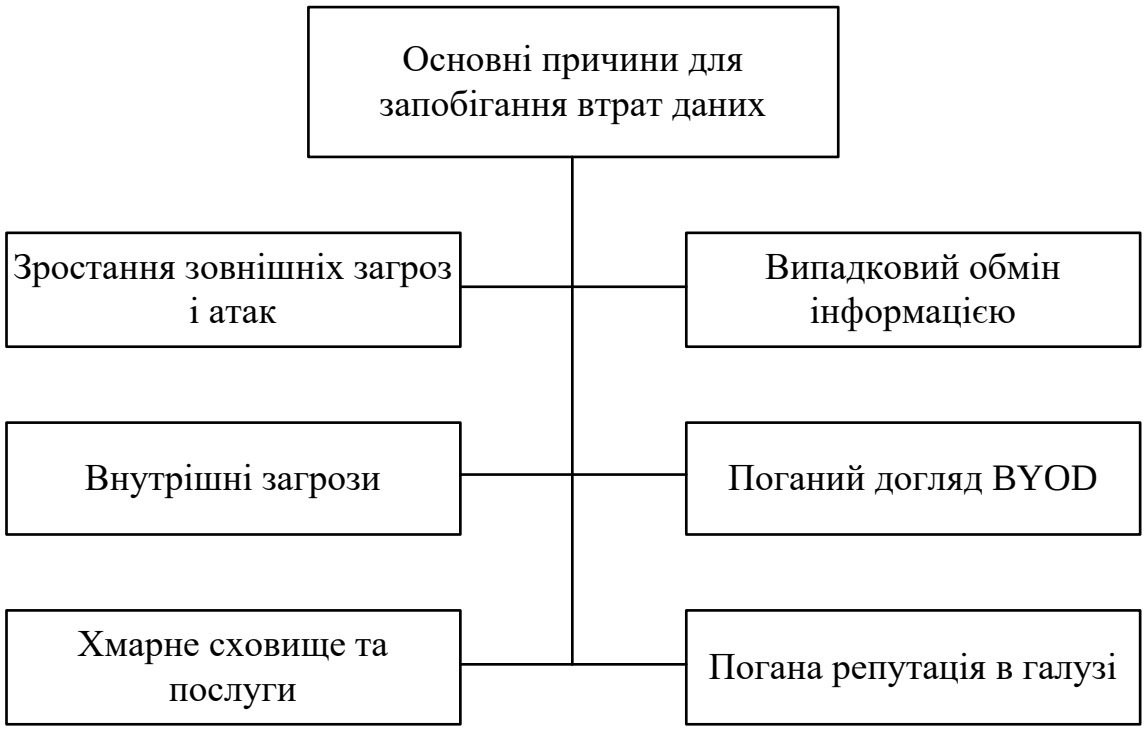

Рисунок 1.1 – Основні причини для запобігання втрат даних

Випадковий обмін інформацією. Особа, про яку йде мова, не може мати наміру завдати шкоди компанії або поставити під загрозу дані компанії. Вони можуть просто стати жертвами соціальної інженерії, найбільш розповсюдженого з методів, які використовують злодії даних [1].

Зловмисник зазвичай вивчає ціль (організацію) і обирає жертву (співробітника) як свій засіб. Звичайна тактика передбачає глибоке вивчення жертви та залучення її до своїх планів, при цьому вона абсолютно не усвідомлює цього.

Вони завжди намагаються, щоб жертва випадково розкрила конфіденційну інформацію, не усвідомлюючи цього.

Поганий догляд BYOD. BYOD (Bring your own device – «принесіть власний пристрій») - це IT-політика, згідно з якою співробітникам компанії дозволено або рекомендується використовувати особисті пристрої для доступу до корпоративних даних та систем компанії. Політика BYOD допомогла багатьом галузям працювати більш ефективно. Існують галузі, які або взагалі не запровадили BYOD, або мають погано розгорнуте та підтримуване рішення BYOD.

З точки зору безпеки, наслідки використання BYOD є надзвичайно серйозними, оскільки BYOD полегшує співробітникам ненавмисне поширення конфіденційної інформації за допомогою персональних мобільних телефонів і планшетів. Вони можуть не знати про рівень безпеки даних, які просто зберігаються у пристрої або під час передачі даних [1]. Втрата даних через BYOD може бути звичайним явищем, коли протоколи безпеки не визначені.

Хмарне сховище та послуги. Співробітники можуть використовувати свої персональні пристрої зберігання даних і персональні онлайн-сервіси, такі як Google Drive або Dropbox, для зберігання та обміну конфіденційною інформацією компанії, яка в жодному випадку не повинна залишатися в мережі та інфраструктурі компанії.

Цілком можливо, особливо в нетехнологічних компаніях, що ці особи не знають про належні протоколи. Відповідальність компанії полягає в тому, щоб забезпечити надійні заходи безпеки мережі, щоб забезпечити співробітникам належні авторизації та дозволи на доступ до даних, а також забезпечити доступ до них лише в мережах компанії.

Погана репутація в галузі. Якщо не має належних заходів безпеки, і в результаті є проблема повторюваних атак, то бізнес може швидко заробити погану репутацію.

Як наслідок можна швидко втратити своїх клієнтів і клієнтів через конкурентів, навіть найлояльніших.

Існують різні технології, що використовуються для захисту інформації (рис. 1.2), більшість з них зосереджені на захисті даних ззовні, а системи DLP зосереджені на захисті даних зсередини.

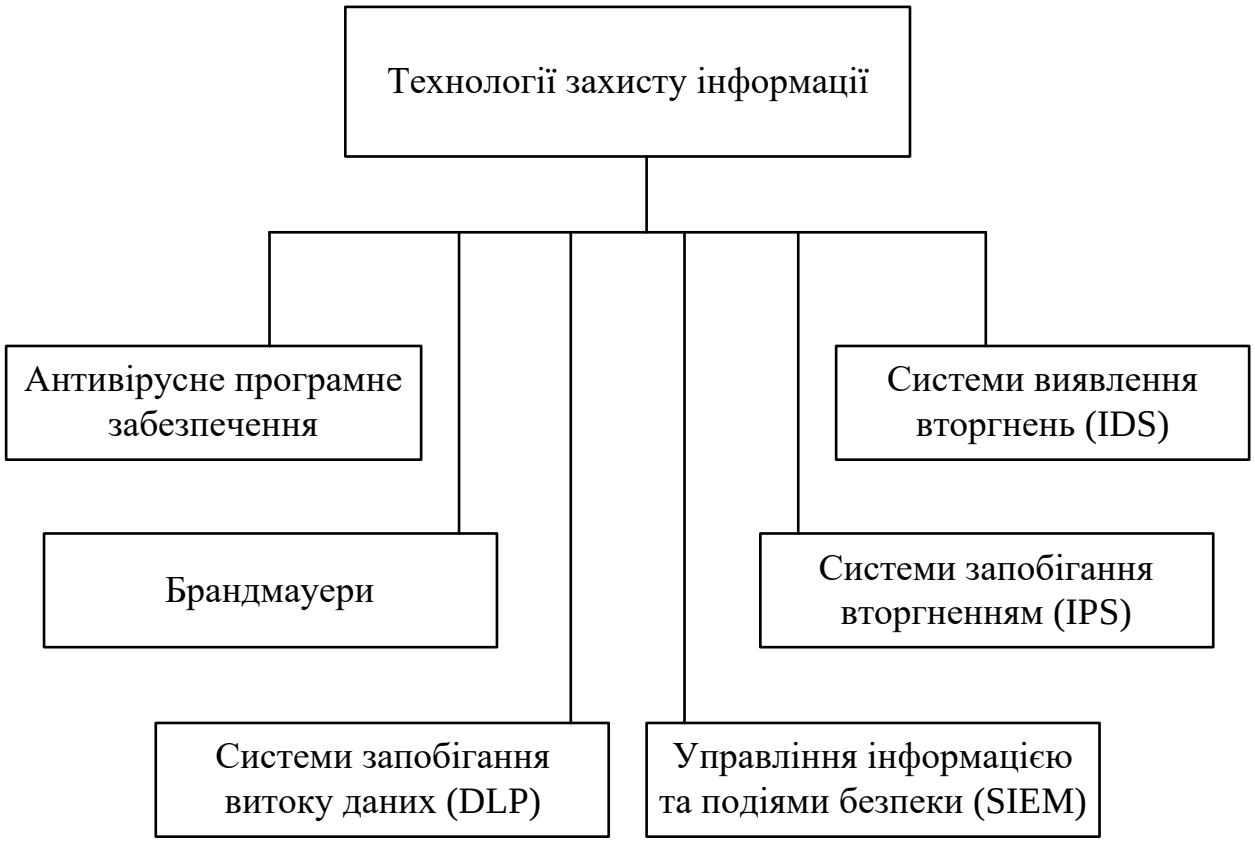

Рисунок 1.2 – Технології захисту інформації

1.2 Системи виявлення та запобігання вторгнень

Системи виявлення вторгнень (Intrusion Detection System, IDS) – це пристрої або програмне забезпечення, яке відстежує мережу чи системну діяльність на предмет виявлення шкідливих дій.

Системи запобігання вторгненням (Intrusion Prevention System, IPS) відстежують мережі, діяльність системи на предмет зловмисних дій, вона в основному ідентифікує зловмисні дії, реєструє інформацію, намагається заблокувати або зупинити дії та повідомляє про дії [3].

Системи IPS є розширенням систем виявлення вторгнень, оскільки обидві вони відстежують мережний трафік, системну діяльність на предмет зловмисної діяльності. IPS здатні запобігати або блокувати виявлені вторгнення. IPS дозволяють виконувати такі дії, як індикація тривоги, залишаючи шкідливі пакети.

Компоненти IDS/IPS поділяють на дві категорії: мережні системи запобігання вторгненню (NIDS/NIPS) і хост-системи (HIDS/HIPS).

NIDS/NIPS перевіряють пакети в мережі та переглядають дані, намагаючись розпізнати атаку. HIDS/HIPS відстежують трафік на одній специфічній системі, HIDS/HIPS відмінно виявляють та запобігають несанкціонованому доступу та активності.

HIDS/HIPS перевіряють стан системи та перевіряють, чи вся поведінка відповідає очікуванням. Як NIDS/NIPS, так і HIDS/HIPS можна використовувати для виявлення атак, відстеження пересування хакерів і попередження адміністратора про поточні атаки.

Більшість IDS/IPS складається з більш ніж однієї програми або апаратного пристрою. IDS/IPS складаються з наступних частин:

- датчики мережі, які виявляють і надсилають дані в системи;

- центральна система моніторингу, що обробляє та аналізує дані, надіслані з датчиків;

- аналіз звіту, який пропонує інформацію про те, як протидіяти певній події;

- база даних, що зберігає IP-адресу та інформацію про зловмисника;

- блок відповідей, що вводить інформацію з попередніх компонентів і формує відповідну відповідь.

Методи IDS/IPS поділяються на два підходи: на основі сигнатур або зіставлення шаблонів. IDS/IPS залежить від бази даних відомих атак. Ці відомі атаки завантажуються в систему як сигнатури.

Найбільшим недоліком систем на основі сигнатур є те, що вони можуть запускатися лише на завантажених сигнатурах. В такому випадку, нова атака може залишитися непоміченою [3].

1.3 Антивірусне програмне забезпечення

Шкідливе програмне забезпечення – це програмне забезпечення, призначене для пошкодження операцій комп’ютера, збору конфіденційних даних та отримання несанкціонованого доступу до комп’ютерної системи. Типом шкідливих програм є віруси, хробаки, трояни, шпигунські програми, бекдори та root-кіт.

Зловмисне програмне забезпечення має дві категорії:

- шкідливе програмне забезпечення, яке змінює такі ресурси, як пам'ять, код BIOS, розширення пристроїв PCI, розширення EEPROMS;

- шкідливе програмне забезпечення, яке не змінює жодного з цих ресурсів, а лише ресурси, які є динамічними за своєю природою, як, наприклад, розділи даних, наприклад, шляхом зміни деяких покажчиків функцій у деяких структурах даних ядра, щоб код зловмисника виконувався замість оригінальної системи чи програми.

Антивірусне програмне забезпечення сканує файл, порівнюючи певні фрагменти коду з інформацією у своїй базі даних, і якщо воно знаходить у базі даних шаблон, що повторює шаблон, він вважається вірусом, і він поміщає на карантин або видаляє цей конкретний файл [4].

Усі програмні файли (виконувані), які надходять в систему, проходять антивірусне сканування. Ті, які відповідають сигнатурам, класифікуються як віруси та занесені до чорного списку. Інші програмні файли потім проходять через Defense + HIPS (система запобігання вторгненню хоста). Тут буде дозволено введення відомих файлів і вони запускатимуться в системі, а невідомі, незалежно від того, хороші вони чи погані, надсилаються до пісочниці Defense+. Їм буде дозволено працювати, але лише в цьому обмеженому середовищі. Ті, які користувач дозволить як безпечні файли, будуть додані до білого списку, а всі інші залишаться в пісочниці, після чого вони відправляться в лабораторії Comodo для аналізу.

1.4 Управління інформацією та подіями безпеки

Системи управління інформацією та подіями безпеки (SIEM) – це програмне рішення, яке об’єднує та аналізує діяльність з багатьох різних ресурсів у всій IT-інфраструктурі компанії.

SIEM збирає дані безпеки з мережних пристроїв, серверів, контролерів домену тощо. SIEM зберігає, нормалізує, об’єднує та застосовує аналітику до цих даних, щоб виявляти тенденції, виявляти загрози та дозволяти організаціям досліджувати будь-які сповіщення [5].

Рішення SIEM є популярним вибором для організацій, які мають різні форми відповідності нормативним вимогам. Завдяки автоматизованому збору й аналізу даних, які він забезпечує, SIEM є цінним інструментом для збору та перевірки даних про відповідність у всій бізнес-інфраструктурі. Рішення SIEM можуть генерувати звіти про відповідність у режимі реального часу для PCI-DSS, GDPR, HIPPA, SOX та інших стандартів відповідності, зменшуючи тягар

управління безпекою та завчасно виявляючи потенційні порушення, щоб їх можна було усунути. Багато рішень SIEM мають готові доповнення, які можуть створювати автоматизовані звіти, розроблені відповідно до вимог.

1.5 Брандмауери

Брандмауер – це інструмент, який допомагає захистити персольні комп’ютери від шкідливого або непотрібного мережного трафіку та запобігти доступу шкідливого програмного забезпечення до персональної мережі. На рис. 1.3 наведено принципову схема брандмауера [6].

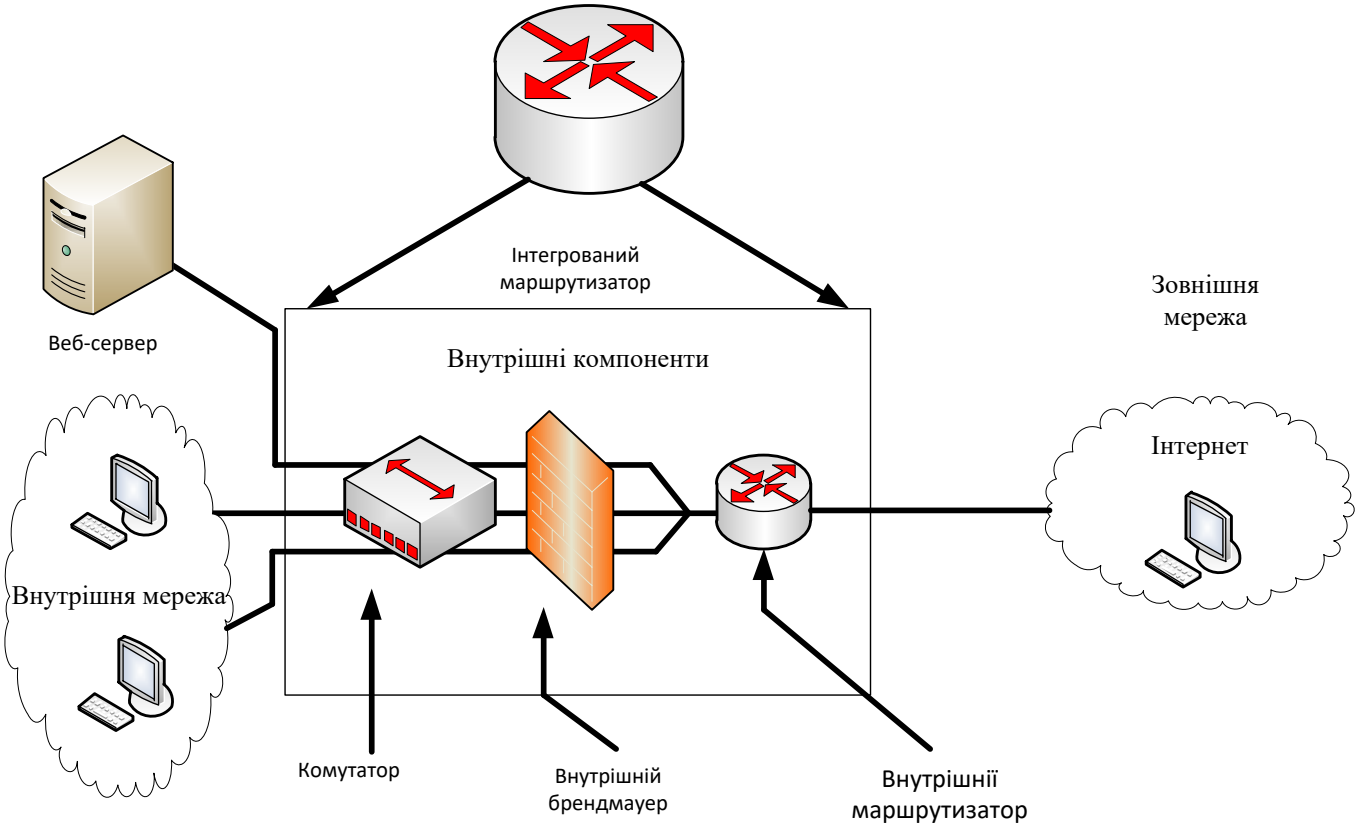

Рисунок 1.3 – Принципова схема брендмауера

Брандмауери захищають комп’ютери різними способами. На рис.1.4 наведено п'ять основних типів брандмауерів.

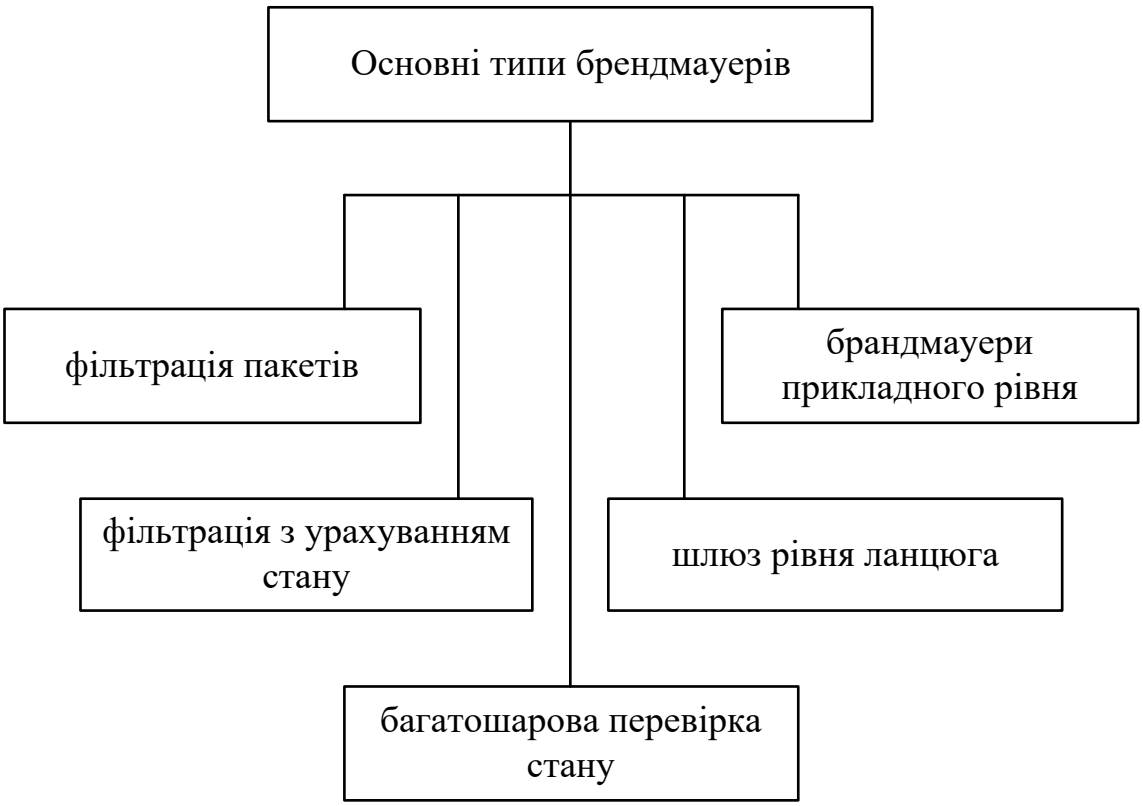

Рисунок 1.4 – Основні типи брендмауерів

Брандмауери існують як у програмній, так і в апаратній формі. Апаратний брандмауер також відомий як мережний брандмауер. Це зовнішній пристрій, який розміщується між комп’ютером та підключенням до Інтернету. Апаратні брандмауери можуть бути корисними для захисту сукупності комп’ютерів, що робить їх особливо цінними для компаній з кількома або більше пристроями. Програмні брандмауери завантажуються на комп’ютер для забезпечення захисту. Програмні брандмауери можуть бути корисними для контролю конкретної мережної поведінки окремих програм у системі, однак одного лише програмного брандмауера може бути недостатньо.

2 ОСНОВНІ ХАРАКТЕРИСТИКИ DLP-СИСТЕМ

2.1 Технологія запобігання витоку даних

Запобігання витоку (втрати) даних (DLP) – це набір продуктів, стратегій, технологій і методів, які гарантують, що кінцеві користувачі не передають критичні чи конфіденційні дані за межі організації. DLP також відноситься до програмного забезпечення для запобігання втрати даних та інших засобів запобігання втрати даних, які допомагають адміністраторам мережі керувати передачею даних кінцевими користувачами.

DLP – це пакет процесів та інструментів, призначених для того, щоб неавторизовані користувачі не отримували доступу до важливої інформації, не використовували її або не втратили.

Інструменти запобігання втраті даних і програмне забезпечення фільтрують потоки даних у мережах, контролюють і відстежують діяльність кінцевої точки, а також відстежують дані в хмарі. Таким чином, різні інструменти DLP захищають дані, які використовуються, передаються мережами або зберігаються (знаходяться в стані спокою). Програми DLP також містять звіти, які допомагають як у виявленні аномалій і проблем для судово-медичної експертизи, так і у виконанні вимог аудиту та рутинної відповідності.

Сьогодні існує широкий спектр рішень DLP для запобігання витоку та втрат даних. Насамперед це пов’язано з багатьма способами існування конфіденційних даних. Інформація знаходиться в багатьох місцях, таких як бази даних, флеш-накопичувачі, файлові сервери, мобільні пристрої, ПК, фізичні сервери, пристрої точки продажу (POS), віртуальні сервери тощо. Також існують різні точки доступу до мережі для переміщення даних, включаючи VPN та бездротові мережі, тому існує багато способів подолати проблеми витоку та втрати даних [7].

2.2 Основні функції DLP систем

Основні функції систем захисту від витоків наведено на рис. 2.1.

Рисунок 2.1 – Основні функції систем захисту від витоків

Насамперед слід визначити дані, переміщення яких контролюватиметься системою, "пред'явити" їх системі з використанням методів, описаних вище, та виявити її реакцію на виявлені інциденти. Важливі також і параметри реакції на інцидент – чи передбачає вона блокування будь-якої операції: відправлення електронного листа, створення екранної копії документа, що захищається, запис даних на USB накопичувач. Незалежно від блокування, майже завжди в журнал системи заноситься максимально детальна предметна інформація про інцидент.

Необхідно також описати правила інформування про інцидент наступним особам:

- співробітнику підрозділу, який відповідає за забезпечення інформаційної безпеки;

- особі, яка є власником інформації;

- підозрюваному у спробі організації витоку.

У разі протидії витокам з використанням мережного сценарію, DLP-система дозволяє здійснювати перехоплення (блокування) або дзерклювання

(тільки аудит) відправлення, проводити аналіз вмісту відправки відповідно до механізмів контролю. Потім при виявленні підозрілого змісту відбувається інформування відповідального співробітника, а деталі інциденту заносяться до журналу системи. Надсилання може бути призупинено, якщо схема підключення DLP-модуля дозволяє це зробити. Більшість DLP-систем передбачає повторну доставку затриманих раніше повідомлень. Призначений співробітник оцінює, наскільки адекватним був вердикт системи і якщо тривога виявляється помилковою, вручну віддає команду провести відправку затриманого повідомлення [8].

2.3 Переваги та недоліки DLP-систем

DLP-системи мають ряд переваг та недоліків. Переваги DLP-систем наведено на рис. 2.2, а недоліки DLP-систем наведено на рис. 2.3.

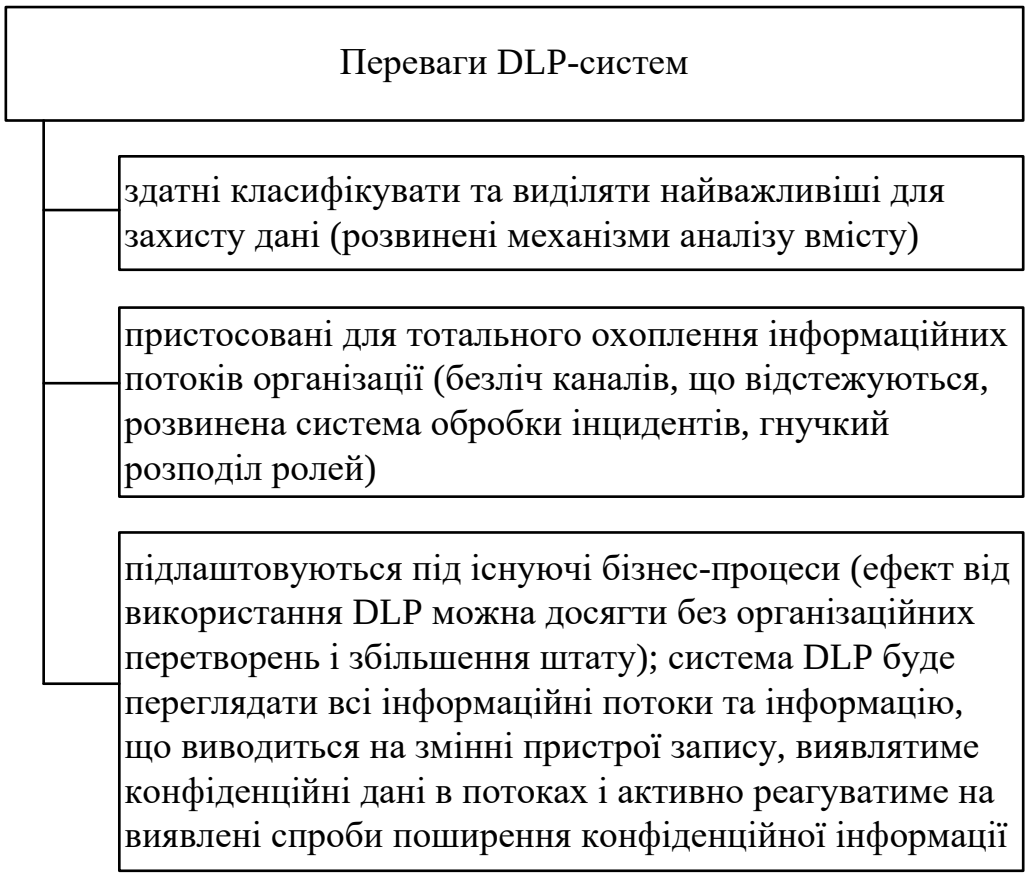

Рисунок 2.2 – Переваги DLP-систем

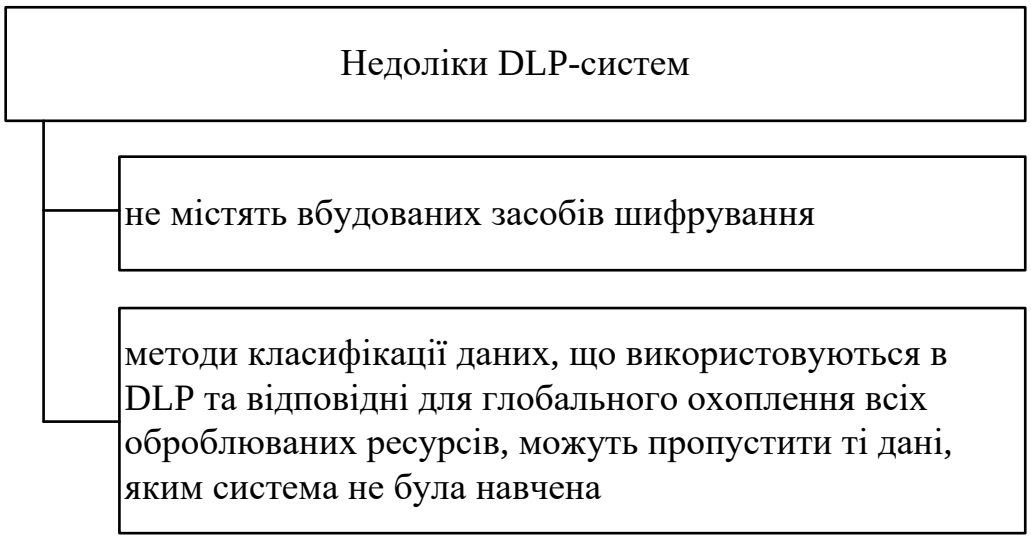

Рисунок 2.3 – Недоліки DLP-систем

3 АНАЛІЗ СТАНІВ DLP-СИСТЕМИ

Метою DLP-систем є захист від витоку інформації протягом усього її життєвого циклу. На рис. 3.1 наведено три основні інформаційні стани:

- Data At Rest – інформація зберігається (знаходиться в стані спокою);
- Data In Motion – інформація передається в мережі;
- Data In Use – інформація використовується (обробляється).

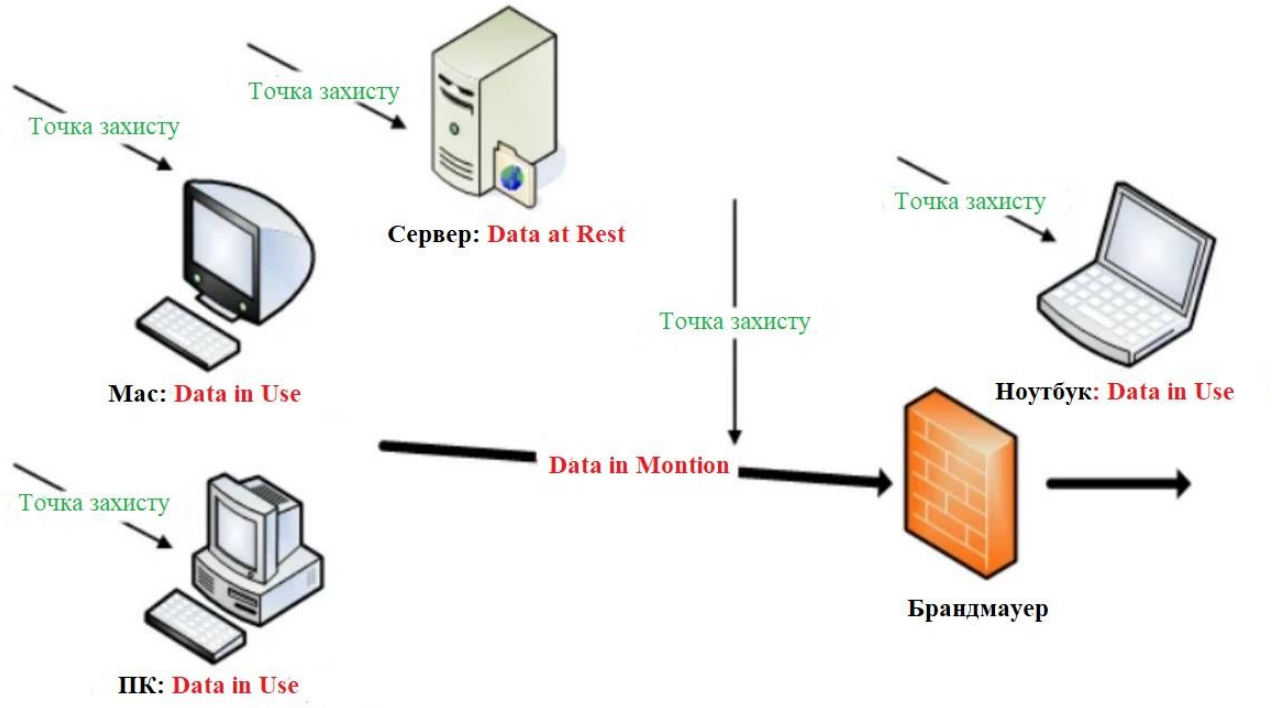

Рисунок 3.1 – Інформаційні стани DLP-систем

Data At Rest включає сканування сховищ та інших сховищ вмісту, щоб визначити, де знаходиться конфіденційний вміст. Це називається виявленням вмісту. Наприклад, можна використовувати продукт DLP для сканування серверів та ідентифікації документів з номерами кредитних карток. Якщо сервер не авторизований для такого типу даних, файл можна зашифрувати або видалити, або власнику файлу надіслати попередження.

Data In Motion – це перевірка трафіку в мережі (пасивно або вбудована через проксі-сервер) для ідентифікації вмісту, що надсилається через певні канали зв’язку. Наприклад, це включає перевірку електронних листів, миттєвих повідомлень та веб-трафіку для фрагментів конфіденційного вихідного коду.

Інструменти In motion часто можуть блокувати на основі центральних політик, залежно від типу трафіку [9].

Data In Use зазвичай обробляються рішеннями кінцевої точки, які відстежують дані під час взаємодії користувача з ними. Наприклад, вони можуть визначити, коли ви намагаєтеся перенести конфіденційний документ на USB-накопичувач і заблокувати його (на відміну від повного блокування використання USB-накопичувача). Інструменти, що використовуються, також можуть виявляти такі речі, як копіювання та вставлення, або використання конфіденційних даних у несанкціонованому додатку (наприклад, хтось намагається зашифрувати дані, щоб прокрастися через датчики).

3.1 Стан Data In Motion

Data In Motion – це стан, коли дані в русі, тобто дані передаються по мережі. Найбільші загрози для даних у русі – це перехоплення та зміна. Наприклад, ім’я користувача та пароль ніколи не повинні передаватися через мережу без захисту, оскільки вони можуть бути перехоплені та використані кимось, щоб видавати себе за іншого або отримати доступ до конфіденційної інформації. Інша особиста інформація, така як інформація про банківський рахунок, також повинна бути захищена при передачі через мережу. Тільки коли мережний сеанс зашифрований, можна не надто сильно турбуватися про те, що дані будуть скомпрометовані під час їх передачі [10].

Дані в русі особливо вразливі для зловмисників, оскільки зловмиснику не обов’язково перебувати поблизу комп’ютера, на якому зберігаються дані, а лише десь на шляху. Тунелі шифрування можуть захистити дані на шляху передачі даних. Схему стану Data In Motion наведено на рисунку 3.2

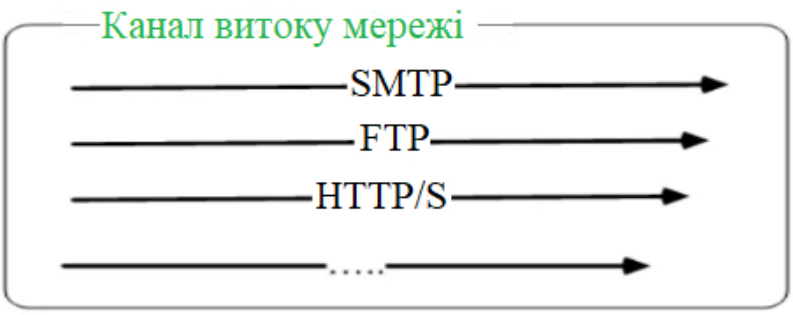

Рисунок 3.2 – Схема стану Data In Motion

3.1.1 Моніторинг мережі

В основі більшості рішень DLP лежить пасивний мережний моніторинг (рис. 3.3). Компонент моніторингу мережі зазвичай розгортається біля або поблизу шлюзу на порту SPAN. Він виконує повне захоплення пакетів, реконструкцію сеансу та аналіз вмісту в режимі реального часу. Але певні організації вимагають повної продуктивності гігабітного Ethernet, хоча цей рівень продуктивності не є необхідним, за винятком дуже незвичайних обставин, оскільки небагато організацій дійсно використовують такий високий рівень комунікаційного трафіку [5].

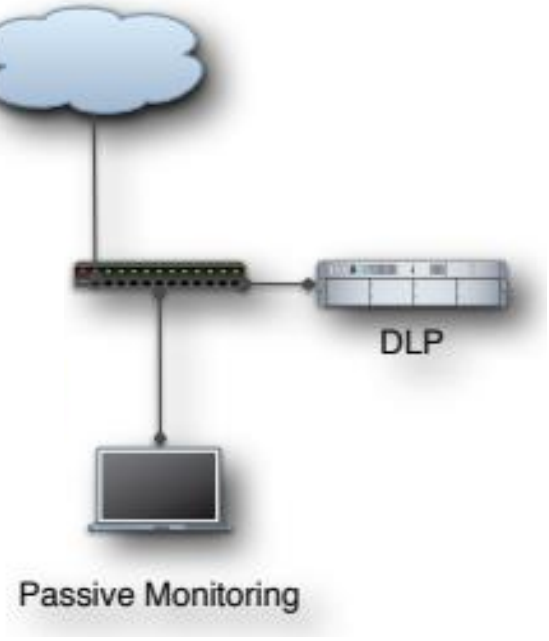

Рисунок 3.3 – Пасивний мережний моніторинг

DLP – це інструмент для моніторингу спілкування співробітників, а не трафіку веб-додатків. Зазвичай малі підприємства працюють зі швидкістю відповідного трафіку менше 50 Мбайт/с, середні підприємства працюють ближче до 50-200 МБ/с, а великі підприємства – близько 300 МБ/с (у деяких випадках, можливо, до 500) [9]. Через накладні витрати на аналіз вмісту не кожен продукт виконує повне захоплення пакетів. Тому доводиться вибирати між попередньою фільтрацією (і, таким чином, відсутністю нестандартного

трафіку) або придбанням додаткових блоків і балансуванням навантаження. Крім того, деякі продукти блокують моніторинг на попередньо визначені комбінації портів і протоколів, а не використовують ідентифікацію служби/каналу на основі вмісту пакетів. Навіть якщо включено повну ідентифікацію каналу програми, потрібно переконатися, що вона ввімкнена. Інакше можна пропустити нестандартні комунікації, наприклад підключення через незвичайний порт [5]. Більшість мережних моніторів є спеціалізованим серверним обладнанням загального призначення зі встановленим програмним забезпеченням DLP. Деякі постачальники використовують справжні спеціалізовані пристрої. Хоча деякі продукти мають свої функції керування, робочого процесу та звітності, вбудовані в мережний моніторинг, вони часто передаються на окремий сервер або пристрій.

3.1.2 Інтеграція електронної пошти

Наступним важливим компонентом є інтеграція електронної пошти (рис. 3.4).

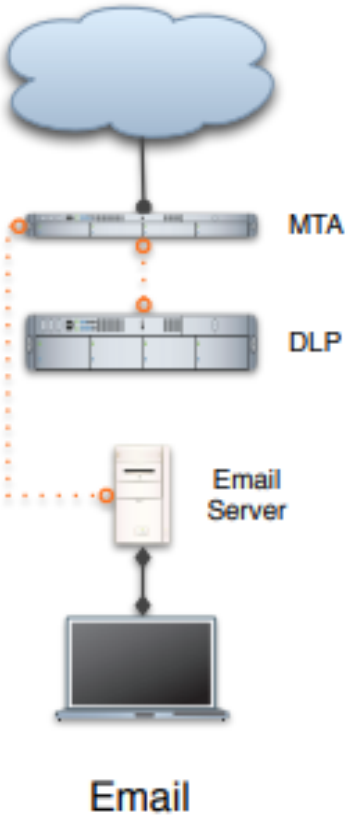

Рисунок 3.4 – Інтеграція електронної пошти

Оскільки електронна пошта зберігається і пересилається, можна отримати багато можливостей, включаючи карантин, інтеграцію шифрування та фільтрацію, без тих самих перешкод, щоб уникнути блокування синхронного трафіку. Більшість продуктів вбудовують MTA (Mail Transfer Agent – агент транспортування пошти) у продукт, що дозволяє просто додати його як інший крок у ланцюжку електронної пошти. Багато з них також безпосередньо інтегруються з деякими з основних існуючих рішень щодо безпеки електронної пошти та для підвищення продуктивності електронної пошти. Одним з недоліків цього підходу є те, що він не дає доступу до внутрішньої електронної пошти. Перебуваючи на сервері Exchange, внутрішні повідомлення ніколи не проходять через зовнішній MTA, оскільки немає причин надсилати цей трафік. Щоб контролювати внутрішню пошту, знадобиться пряма інтеграція Exchange/Lotus, що рідко зустрічається на ринку. Повна інтеграція відрізняється від простого сканування журналів/бібліотек після факту, що деякі компанії називають внутрішньою підтримкою пошти. Хороша інтеграція електронної пошти є абсолютно важливою, якщо застосовувати фільтрацію, а не просто моніторинг [9].

3.1.3 Фільтрація, блокування та інтеграція проксі

Майже кожен, хто впроваджує рішення DLP, зрештою захоче почати блокувати трафік. Але блокування – це складна річ, тим більше, що необхідно дозволити хороший трафік, блокувати лише поганий трафік і приймати рішення за допомогою аналізу вмісту в реальному часі. Електронну пошту досить легко фільтрувати. Це не зовсім у реальному часі і є проксі за своєю природою. Додавання ще одного переходу аналізу є проблемою, яку можна вирішити навіть у найскладніших середовищах. Поза електронною поштою більшість комунікаційного трафіку відбувається синхронно – все виконується в режимі реального часу. Таким чином, якщо необхідно відфільтрувати його, потрібно або перекрити трафік, або заразити його ззовні.

У випадку з мостом маємо систему з двома мережними картами, яка виконує аналіз контенту посередині. Якщо є щось погане, міст розриває з’єднання для цього сеансу. Перемикання – не найкращий підхід для DLP, оскільки він може не зупинити весь поганий трафік до того, як він витікає. Дуже небагато продуктів використовують цей підхід, хоча він має перевагу, що

не залежить від протоколу [9].

Проксі залежить від протоколу/програми і збирає трафік перед його передачею, що дозволяє глибше аналізувати. Проксі-шлюзи переважно для протоколів HTTP, FTP та IM. Деякі рішення DLP включають власні проксі; вони, як правило, інтегруються з існуючими постачальниками шлюзів/проксі, оскільки більшість клієнтів віддають перевагу інтеграції з цими існуючими інструментами. Інтеграція веб-шлюзів зазвичай здійснюється за допомогою протоколу iCAP, що дозволяє проксі-серверу захоплювати трафік, надсилати його системі DLP для аналізу та обривати зв'язок, якщо є порушення. Це означає, що не потрібно додавати інше обладнання перед мережним трафіком, а постачальники DLP можуть уникнути труднощів створення спеціального мережного обладнання для вбудованого аналізу. Якщо шлюз містить зворотний проксі-сервер SSL, також можна перевіряти з'єднання SSL. Потрібно буде внести зміни на кінцевих точках, щоб працювати з усіма сповіщеннями про сертифікати, але тепер можна заглянути в зашифрований трафік. Для обміну миттєвими повідомленнями знадобиться проксі-сервер миттєвих повідомлень і продукт DLP, який спеціально підтримує будь-який протокол миттєвих повідомлень, який використовується [9].

Схема фільтрації, блокування та інтеграції проксі наведено на рис. 3.5.

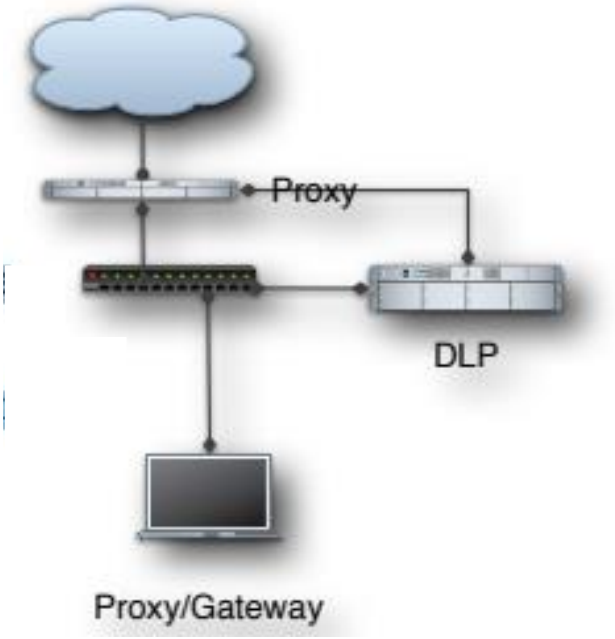

Рисунок 3.5 – Фільтрація, блокування та інтеграція проксі

Спосіб фільтрації TCP Poisoning (отруєння TCP) відстежує трафік, і коли бачите щось погане, вводить пакет скидання TCP, щоб знищити з'єднання. Це працює на кожному протоколі TCP, але не дуже ефективно. По-перше, деякі протоколи будуть продовжувати намагатися пропустити трафік. Якщо відбувається TCP отруєння одного повідомлення електронної пошти, сервер намагатиметься надіслати його протягом 3 днів, кожні 15 хвилин. Інша проблема така ж, як і перемикання – оскільки взагалі не ставиться в чергу трафік, до того часу, коли можна помітити щось погане, може бути надто пізно. Це хороший проміжок, щоб охопити нестандартні протоколи, але потрібно якомога більше проксі.

3.1.4 Внутрішні мережі

Технічно DLP-системи здатні контролювати внутрішні мережі, DLP рідко використовується для внутрішнього трафіку, крім електронної пошти. Шлюзи забезпечують зручні точки дроселя. Внутрішній моніторинг – це найкраща перспектива з огляду на вартість, ефективність та управління політикою. Деякі постачальники DLP мають партнерські відносини для внутрішнього моніторингу, але для більшості організацій ця функція є менш пріоритетною [9].

3.1.5 Розподілені та ієрархічні розгортання

Усі середні та великі підприємства, а також багато малих організацій мають кілька місць розташування та веб-шлюзи. Рішення DLP має підтримувати кілька точок моніторингу, включаючи комбінацію пасивного моніторингу мережі, проксі-точки, сервери електронної пошти та віддалених місць. Хоча обробку та аналіз можна розвантажити до віддалених точок застосування, вони повинні надсилати всі події назад на центральний сервер керування для робочого процесу, звітності, розслідування та архівування. Віддалені офіси зазвичай легко підтримувати, оскільки можна просто знизити політику звітування, але не кожен продукт має таку можливість.

Більш просунуті продукти підтримують ієрархічні розгортання для організацій, які хочуть керувати DLP по-різному в кількох географічних місцях або за бізнес-підрозділом. Міжнародним компаніям це часто потрібно для

виконання вимог законодавства щодо моніторингу, які відрізняються в залежності від країни. Ієрархічне управління підтримує скоординовану локальну політику та застосування в різних регіонах, працює на власних серверах керування, зв'язуючись із центральним сервером керування. Ранні продукти підтримували лише один сервер керування, але тепер існують варіанти вирішення цих розподілених ситуацій за допомогою поєднання корпоративних/регіональних/підприємницьких політик, звітності та робочого процесу.

3.2 Стан Data at Rest

Документація вважається безпечною в стані спокою, якщо вона зашифрована (тому для її розшифровки потрібна непрацездатна кількість часу під час атаки грубої сили), ключ шифрування не міститься на тому самому носії даних, а ключ має достатню довжину і рівень випадковості, щоб зробити його несприйнятливим до атаки словника [11].

На рис. 3.6 наведено схему стану Data at Rest.

Рисунок 3.6 – Схема стану Data at Rest

Існують різні технології захисту інформації в стані Data at Rest. Перелік цих технологій наведено на рис. 3.7.

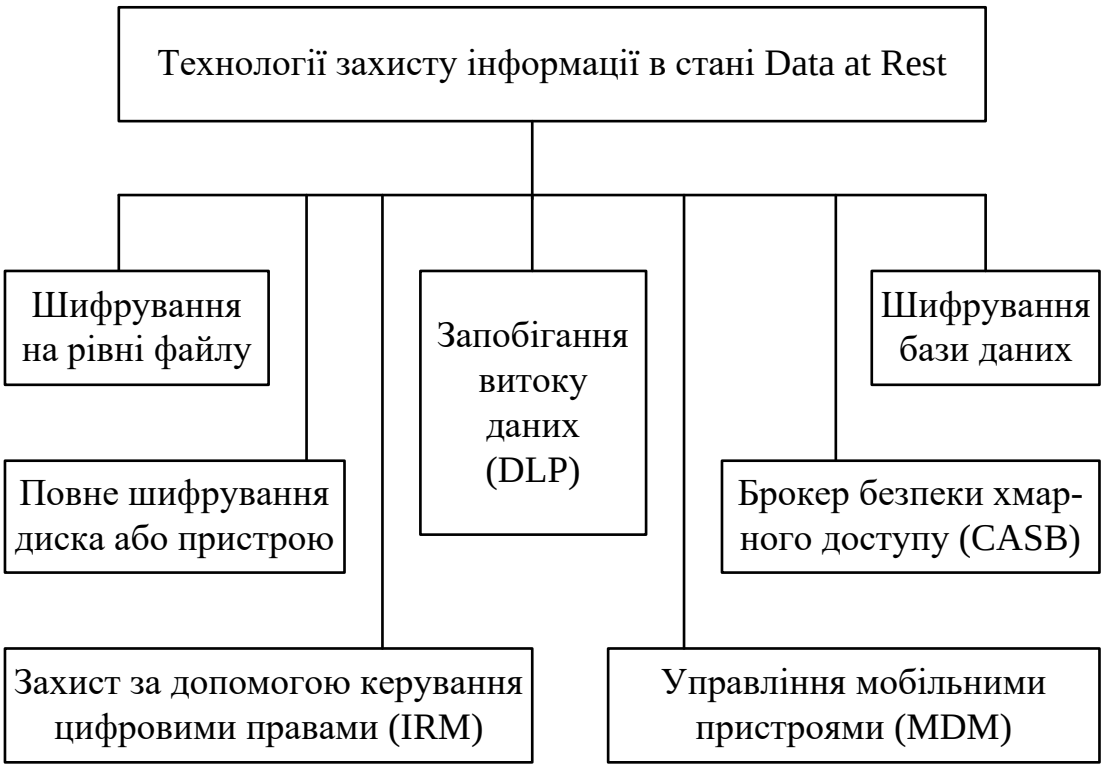

Рисунок 3.7 – Технології захисту інформації в стані Data at Rest

Повне шифрування жорсткого диска або пристрою дозволяє, наприклад, у разі втрати ноутбука або комп'ютера не отримати доступ до даних, що містяться на ньому, просто підключивши жорсткий диск або пристрій в іншу машину. Його перевага полягає в тому, що він «прозорий» для користувача, оскільки, якщо користувач увійшов правильно, він або вона може отримати доступ до документів так само, як і на незашифрованому комп'ютері. Однак, якщо комп'ютер або файловий сервер доступні адміністратору, ніщо не завадить недобросовісному користувачеві отримати доступ до даних, скопіювати їх, повторно надіслати тощо. Дані захищені під час перебування на пристрої чи жорсткому диску, але більше не є захищеними, якщо їх вилучити з пристрою (скопіювати на інший пристрій, надіслати повторно тощо).

При шифруванні на рівні файлу жоден розділ або жорсткий диск не шифруються, лише окремі файли. Шифрування з відкритим ключем або симетричне шифрування дозволяє, наприклад, шифрувати файли. Файли не тільки шифруються, коли вони зберігаються на диску, але також можуть бути захищені під час транспортування, коли вони надсилаються, наприклад, як вкладення в електронному листі. У цьому випадку втрачається прозорий доступ користувача, а також прозорий захист користувача. Тобто з PGP, наприклад,

необхідно мати відкритий ключ особи, з якою необхідно поділитися захищеним файлом, а з іншого боку, вона повинна мати відкритий ключ, щоб мати можливість його розшифрувати. З іншого боку, як тільки документ був розшифрований одержувачем, його можна зберегти незахищеним, надіслати незахищеним тощо [11].

Шифрування бази даних: такі системи баз даних, як SQL Server або Oracle, використовують TDE – прозоре шифрування даних для захисту даних, що зберігаються в базах даних. Технології TDE виконують операції шифрування та дешифрування даних і файлів журналів у режимі реального часу. Це дозволяє розробникам додатків, наприклад, працювати із зашифрованими даними за допомогою AES або 3DES, наприклад, без необхідності змінювати існуючі програми. Цей тип шифрування захищає дані, які зберігаються в базі даних, але не тоді, коли відповідна програма вже отримала доступ до даних і їх можна вилучити.

Захист за допомогою керування цифровими правами (IRM) – технології керування правами на дані, як управління правами на інформацію (SealPath), дозволяють шифрувати документацію, застосовуючи до неї постійний захист. Документація в стані спокою зашифрована і доступна лише користувачам, які мають до неї права доступу. На відміну від шифрування на рівні файлу, користувач, який отримує, може отримати до нього доступ, щоб прочитати і навіть змінити його, але не може повністю розшифрувати файл (якщо йому не було призначено повний контроль над файлом).

Управління мобільними пристроями (MDM) – один із способів керування даними на мобільних пристроях. Інструменти MDM дозволяють обмежувати доступ до певних корпоративних програм, блокувати доступ до пристрою або шифрувати дані на мобільному телефоні чи планшеті. Як і у випадку зі стандартним шифруванням, вони корисні на випадок втрати пристрою, але коли дані надсилаються назовні пристрою, вони залишаються незашифрованими.

Системи запобігання витоку даних (DLP) серед інших функцій, дозволяють здійснювати пошук або розташування конфіденційних даних на кінцевій точці або в мережному сховищі. У випадку даних у сховищі вони можуть видалити дані, наприклад, або заблокувати доступ певним користувачам у випадку, якщо вони порушують будь-яку політику безпеки (наприклад, на комп’ютері, якого не повинно бути). Вони дійсні, поки дані

знаходяться всередині організації, але вони не можуть діяти з ними після того, як дані залишили організацію.

Брокери безпеки хмарного доступу (CASB – Cloud Access Security Brokers) – це системи, які дозволяють застосовувати політики безпеки до документації, яка зберігається в хмарних системах, таких як Office 365, Box, Salesforce тощо. Можна сказати, що це система DLP хмарний додаток замість периметра організації. Що стосується неактивних даних, CASB здатні виявляти конфіденційні дані в певних хмарних сховищах даних і застосовувати політику захисту до документації, наприклад, видаляючи загальнодоступне посилання на документ і обмежуючи його групою користувачів, якщо дані визначені. Як і DLP, вони можуть діяти, поки дані знаходяться в хмарі (наприклад, G-Suite), але не після того, як документ покине хмару [11].

Проблеми захисту даних у стані Data at Rest наведено на рис. 3.8

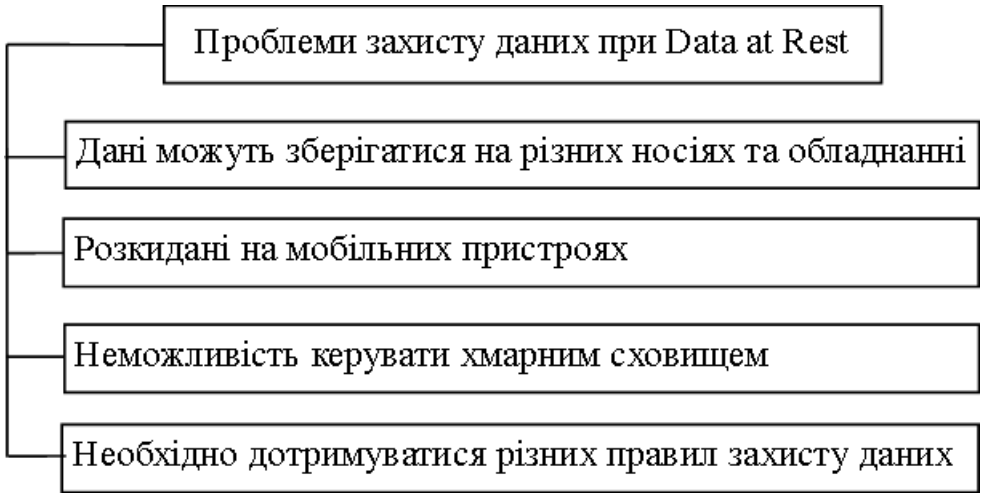

Рисунок 3.8 – Проблеми захисту даних у стані Data at Rest

Інформація може зберігатися на різних носіях та обладнанні тому важлива документація міститься не тільки на файлових серверах або менеджерах документів, але також можуть бути копії на ПК користувачів, USB-пристроях тощо.

Інформація розкидана на мобільних пристроях оскільки мобільні телефони та планшети є ще одним робочим інструментом, який може містити важливу документацію, яку потрібно захищати. Необхідно враховувати, що в багатьох випадках, коли керують конфіденційними даними, мобільні пристрої,

на яких вони виявлені, є не корпоративними, а особистими та непідконтрольними IT-відділам.

Неможливість керувати хмарним сховищем тому багато постачальників сховищ пропонують шифрування та захист даних, якими вони керують у стані спокою. Однак ключі шифрування належать постачальнику сховища, а не компаніям, які їх наймають, тому контроль над документацією, що зберігається в цих хмарах, втрачається.

Необхідно дотримуватися різних правил захисту даних залежно від вертикалі, в якій працює компанія, на неї можуть поширюватися суворі правила щодо захисту та контролю даних. Наприклад, дані пацієнтів у секторі охорони здоров'я або дані клієнтів у фінансовому секторі захищені залежно від території такими правилами, як EU-GDPR, HIPAA, PCI тощо. Ці правила встановлюють політику захисту даних у стані спокою, незалежно від того, чи зберігаються вони в базі даних, на файловому сервері чи на мобільних пристроях.

Щоб подолати ці проблеми, IT-відділи повинні проаналізувати основні ризики, з якими вони стикаються, що стосуються керування своїми даними в стані спокою, і вибрати технологію або технології, віддаючи пріоритет тим, які усунуть або пом'якшать ті, що є найбільш вірогідні та/або мають найбільший вплив на їхню організацію [11].

3.3 Стан Data in Use

Стан Data in Use – це стан, коли дані використовуються або коли до них звертається програма для лікування. Зазвичай за програмою знаходиться користувач, який хоче отримати доступ до даних, щоб переглянути їх, змінити їх тощо. У цьому стані дані є більш вразливими, у тому сенсі, що для того, щоб побачити їх, користувач повинен мати можливість для доступу до розшифрованого вмісту (у випадку, якщо він був зашифрований). На рис. 3.9 наведено схему стану Data in Use.

Щоб захистити дані, що використовуються, зазвичай слід встановлювати засоби керування «перед» доступом до вмісту (рис. 3.10).

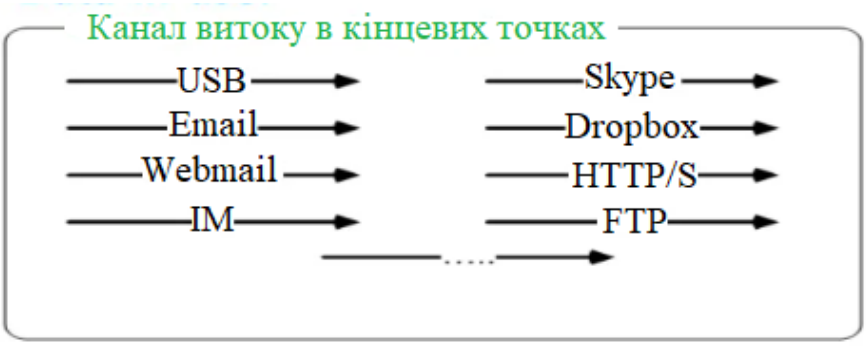

Рисунок 3.9 – Схема стану Data in Use

Рисунок 3.10 – Засоби керування «перед» доступом до вмісту

Інструменти керування ідентифікацією перевіряють, що користувач, який намагається отримати доступ до даних, є тим, за кого він себе видає, і чи не було крадіжки особистих даних. У цих випадках стає все більш важливим захистити доступ до даних за допомогою двофакторної аутентифікації.

Інструменти умовного доступу або контролю доступу на основі ролей (RBAC) надають доступ до даних на основі ролі користувача або інших параметрів, таких як IP, місцезнаходження тощо [11].

Однак у цих випадках захищаючи дані, обмежуючи точніше, хто може, а хто не може отримати до них доступ, але після доступу до бази даних або документа не можна перешкодити особі робити з даними те, що вона хоче.

За допомогою захисту цифрових прав або IRM можна отримати ефективний захист при використанні даних, оскільки можна обмежити дії, які

користувач може виконувати після того, як вони отримали доступ до даних. Наприклад, можна заборонити редагувати, друкувати тощо. Існують хмарні платформи для спільної роботи або менеджери документів, які дозволяють налаштувати контроль цифрових прав, наприклад лише перегляд, запобігання, завантаження тощо. Однак, якщо вже завантажили документ, він є абсолютно незахищеним.

Завдяки захисту IRM, застосованому безпосередньо до файлу (а не до самого менеджера документів чи платформи для співпраці), можна застосувати захист, який переміщується з документами та обмежує дозволи на відкриття, де б він не був. Незалежно від того, чи є дані в хмарі чи були завантажені, можна змусити користувача побачити їх, але не повністю знімати захист, роздрукувати тощо.

У стані Data in Use також існує ряд проблем захисту даних. Більшість інструментів, які контролюють доступ до даних, роблять це перед наданням доступу, але після перевірки, контролювати те, що можна зробити з даними, стає складніше.

Навіть якщо обмежити дозволи на документацію, якщо вона відображається користувачеві в програмі, у програмі перегляду, він завжди може зробити знімок, наприклад, хоча можна пом’якшити цю дію за допомогою динамічних водяних знаків на відкритому документі [11].

Платформи для спільної роботи, які обмежують права, наприклад заборону завантажувати або дозволяти лише перегляд документа, можуть бути ефективними, коли потрібно лише отримати доступ до документа, але мають обмеження, якщо потрібно змінити документ, наприклад, за допомогою гнучкого інструменту на робочому столі. Крім того, не треба забувати, що сама хмарна платформа має документ, розшифрований під час доступу та збережений у своїх системах, щоб технічно отримати доступ до його вмісту. Це може бути проблемою, коли йдеться про конфіденційні дані або дані, що підлягають суворим правилам захисту.

Не вдаючись у питання захисту даних, що використовуються через шифрування даних у пам'яті, поки програма відкрита, щоб уникнути їх дампу, захист цифрових прав або IRM є найефективнішим захистом даних, оскільки він поєднує шифрування, керування дозволами та контроль ідентичності.

Цей захист дозволяє зберігати документацію в безпеці у всіх трьох її станах: Data At Rest, Data In Motion та Data In Use. Захист пересувається з

документом і супроводжує його всюди, куди він подорожує, дозволяючи користувачеві працювати з даними, знаючи, що в разі потреби він не матиме повного контролю над ними [11].

4 ПРОГРАМНІ ЗАСОБИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

4.1 Endpoint Protector by CoSoSys

Компанія CoSoSys пропонує Endpoint Protector як рішення на місці, як хмарну послугу та як окремий пакет програмного забезпечення. Версія на місці захищає комп'ютери під керуванням Windows , Mac OS і Linux . Центральний пристрій Endpoint Protector Server зв'язується по мережі з клієнтським програмним забезпеченням, встановленим на кожній кінцевій точці. Сервер також захищає підключені пристрої, такі як цифрові камери та USB-накопичувачі. Система захисту кінцевих точок також доступна як програмне забезпечення, яке реалізує віртуальний пристрій на приватному власному сервері [12].

Інтерфейс Endpoint Protector by CoSoSys наведено на рис. 4.1.

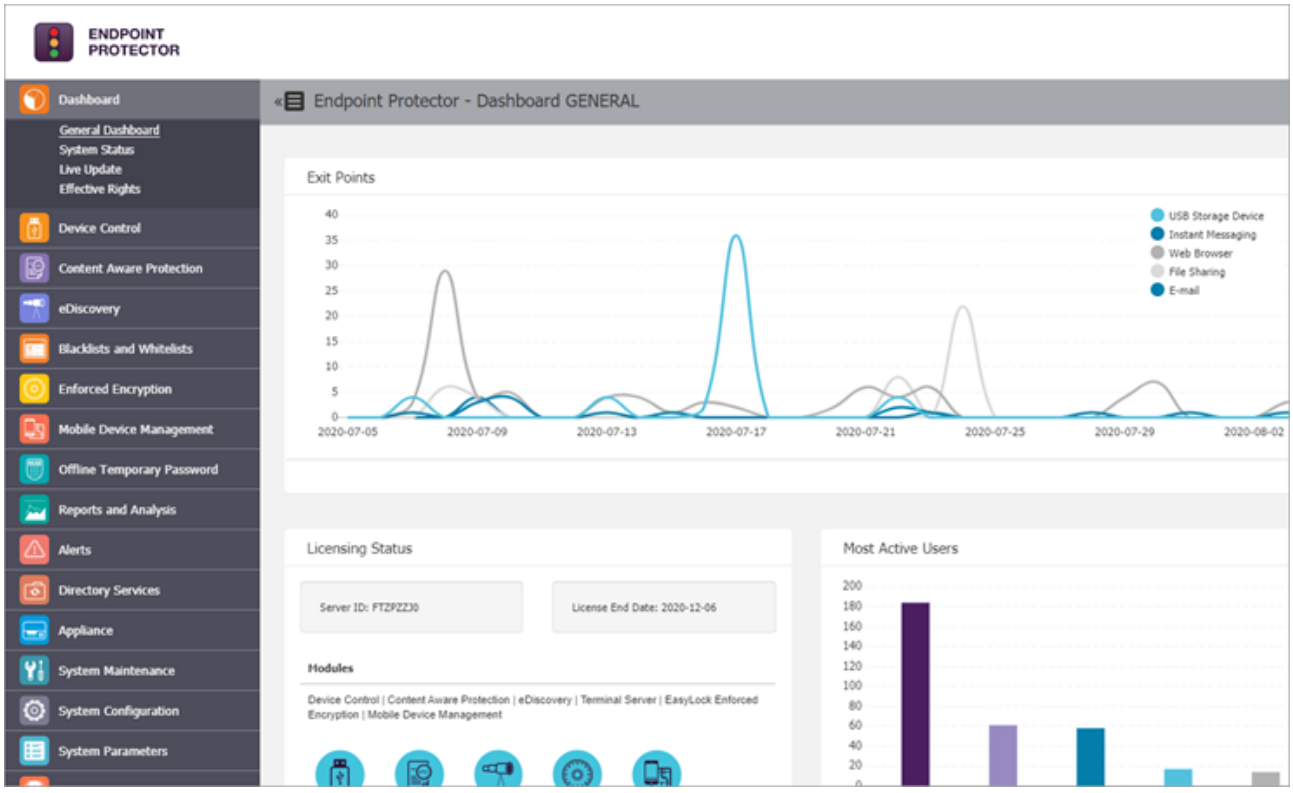

Рисунок 4.1 – Інтерфейс Endpoint Protector by CoSoSys

Основні характеристики Endpoint Protector by CoSoSys:

- платформа захисту кінцевих точок;
- пристрій, локальне програмне забезпечення або хмарний сервіс;
- відповідає вимогам HIPAA, PCI DSS та GDPR;
- також захищає підключені пристрої;
- примусове шифрування.

Повна система Endpoint Protector включає захист вмісту, контроль пристрою, примусове шифрування, виявлення мережі та керування мобільними пристроями. Доступна автономна версія для захисту лише однієї кінцевої точки на інсталяцію. Endpoint Protector Basic включає модулі захисту вмісту та пристроїв

Також є пакети «програмне забезпечення як послуга», замість того, щоб запускати власні хости та програмне забезпечення, можна вибрати My Endpoint Protector. Це включає захист вмісту, керування пристроєм та керування мобільним пристроєм. У всіх реалізаціях система відповідає вимогам HIPAA, PCI DSS та GDPR.

Система захисту вмісту в Endpoint Protector керує передачею файлів відповідно до встановлених адміністратором політик. Усі передачі файлів можна заблокувати для певних груп користувачів або дозволити переміщення конфіденційних файлів, якщо вони відповідають певним критеріям. Аналогічно, система керування пристроєм може або повністю заблокувати пристрої від підключення до захищеної кінцевої точки, або дозволити передачу файлів за певних умов.

4.2 Symantec DLP

Рішення Symantec DLP поєднує відстеження активності користувачів із контролем ризику даних. Він може відстежувати дані, що зберігаються на серверах, настільних комп’ютерах, мобільних пристроях і в хмарному сховищі. Початкова перевірка під час встановлення визначає всі місця, які містять конфіденційні дані, і дає можливість перенести їх всі на центральний сервер керування, у безпечне сховище даних або захистити їх на місці. Внаслідок створюються шаблони та робочі процеси для відповідності стандартам HIPAA , GDPR та PCI DSS.

Інтерфейс Symantec DLP наведено на рис. 4.2.

Рисунок 4.2 – Інтерфейс Symantec DLP

Основні характеристики Symantec DLP:

- відстеження активності користувачів,
- захист шифрування,
- відповідає HIPAA, GDPR та PCI DSS.

Інструмент реєструє весь доступ до конфіденційних даних і відстежує облікові записи, які викликали сповіщення. Конфіденційні документи зашифровані, і їх можуть побачити лише авторизовані користувачі. Інструмент також забезпечує повне знищення відкинутих копій і документів, що вилучені, і в пам’яті не залишаються версії для відновлення. Усі копії відстежуються та зберігаються в безпеці, навіть коли їх надсилають у віддалені місця або на мобільні пристрої, якими володіють користувачі [12].

Symantec DLP містить документи з конфіденційними даними за допомогою шифрування та ідентифікує цільових одержувачів, знімаючи відбитки пальців на кожній копії. Шифрування та ідентифікація доступу поєднуються з обмеженнями на переміщення та копіювання даних. Це дає змогу блокувати файли та дані від вкладення в електронні листи або передавання через мережу чи Інтернет.

Система Symantec DLP є частиною системи захисту кінцевих точок. Він шукає вторгнення та шкідливе програмне забезпечення, яке може поставити під загрозу конфіденційність ваших даних. Система включає моніторинг програмного забезпечення, яке не авторизоване бізнесом, але встановлене на тому ж пристрої, що й конфіденційні дані – ситуація, яка особливо поширена у випадку використання пристроїв, що належать користувачам, для доступу до даних компанії.

4.3 McAfee DLP

Компанія McAfee пропонує комплексне попередження втрати даних в одному пакеті. Він захищає дані в мережі, у хмарі та на кінцевих точках. Може керувати загальними політиками та оптимізувати робочі процеси щодо інцидентів за допомогою гнучких параметрів розгортання.

Інтерфейс McAfee DLP наведено на рис. 4.3.

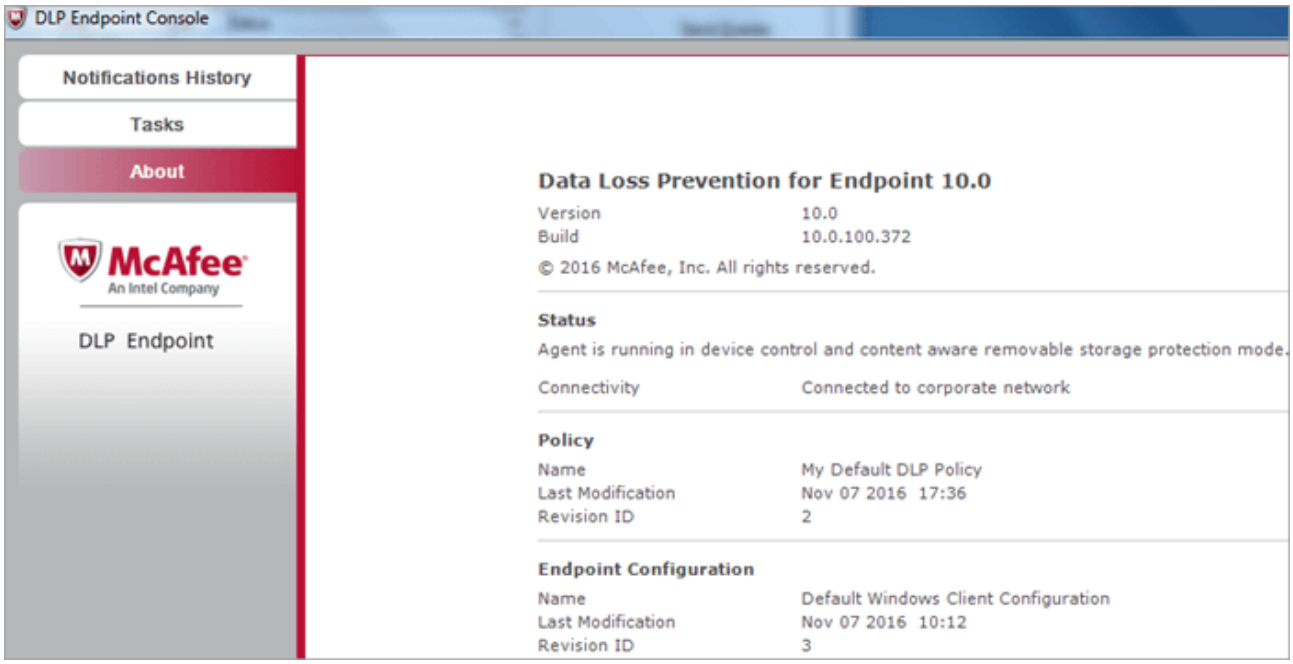

Рисунок 4.3 – Інтерфейс McAfee DLP

Основні характеристики McAfee DLP:

- забезпечує видимість завдяки технології захоплення;
- дає змогу побачити, як дані використовуються та як вони витікають.;
- має більш потужну функцію класифікації даних для ідентифікації та

класифікації даних;

- може шифрувати, перенаправляти, поміщати на карантин або блокувати передачу даних, які порушують політику.

McAfee DLP забезпечує централізоване управління інцидентами та звітність. Ваші локальні та хмарні політики DLP будуть синхронізовані McAfee.

4.4 Forcepoint DLP

Forcepoint забезпечує індивідуальний та адаптивний захист даних. Це дозволяє блокувати дії лише тоді, коли це необхідно, і, отже, допомагає підвищити продуктивність. Забезпечує відповідність нормативним вимогам у понад 80 країнах щодо GDPR, CCPA тощо. Це автоматично запобігає порушення даних.

Інтерфейс Forcepoint DLP наведено на рис. 4.4.

Forcepoint має велику попередньо визначену бібліотеку політик для перегляду та контролю всіх ваших даних. За допомогою Forcepoint можна захистити PII та PHI, фінансові дані компанії, комерційні таємниці, дані кредитних карток тощо навіть у зображеннях. Це дозволяє стежити за інтелектуальною власністю як у структурованих, так і в неструктурованих формах [13].

Основні характеристики Forcepoint DLP:

- для захисту даних Forcepoint надає функції Drip DLP, Native Remediation, комплексне виявлення даних і OCR;

- забезпечує власну поведінкову аналітику, захист, адаптований до ризику, та застосування політики на основі ризиків;

- має функції для запобігання повільної крадіжки даних, навіть якщо пристрої користувача знаходяться поза мережею;

- гнучкість бази даних.

Інструмент Forcepoint простий у використанні і може захистити ваші дані скрізь. Він зменшив гучність сповіщень, помилкові спрацьовування та сигнали тривоги, і, отже, користувач зможе зосередитися на тому, що важливо.

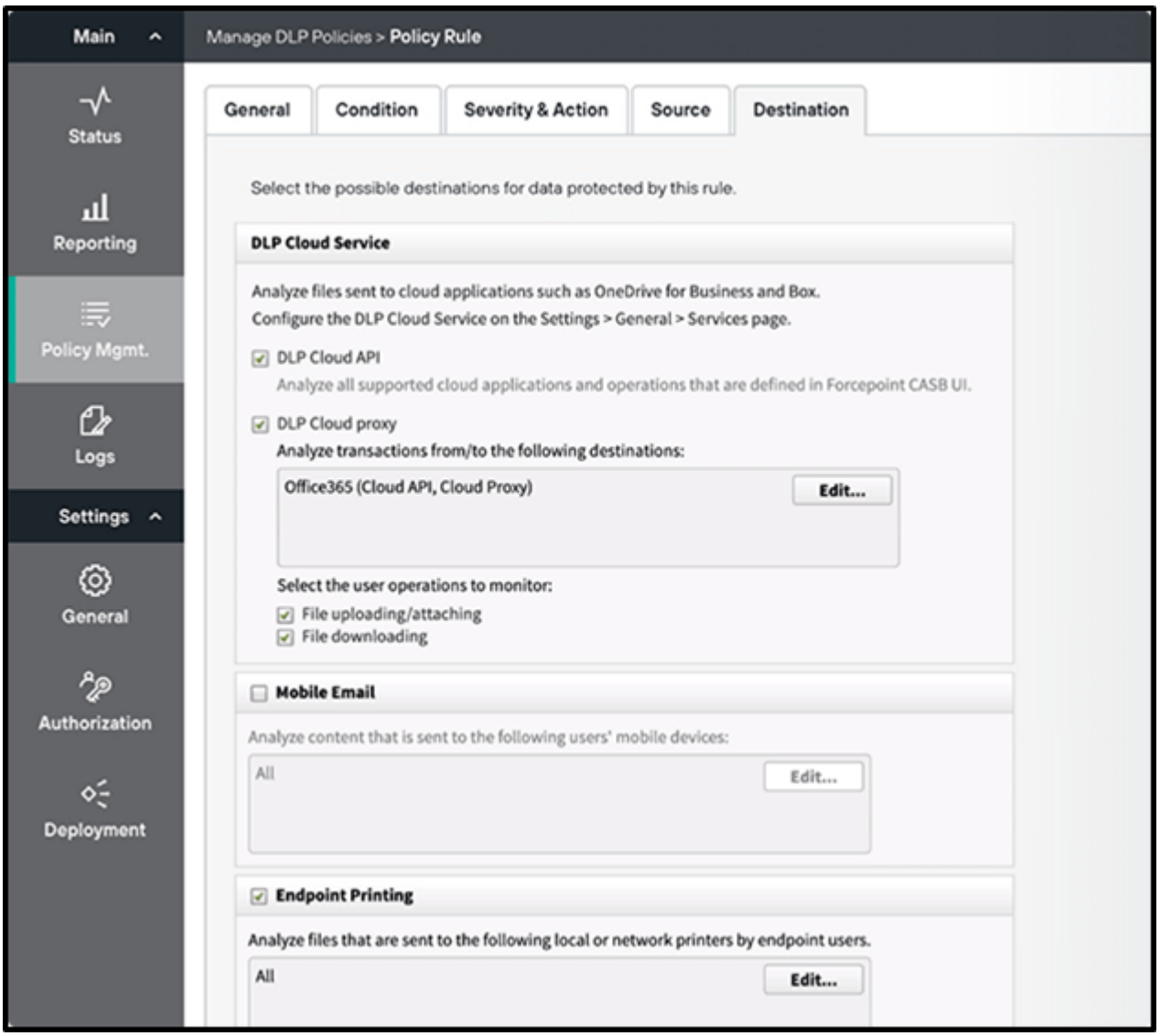

Рисунок 4.4 – Інтерфейс Forcepoint DLP

4.5 SecureTrust DLP

SecureTrust DLP – це рішення для виявлення, моніторингу та захисту даних у стані спокою, у русі й у використанні. Інструмент запобігає ексфільтрації та забезпечить відповідність нормативним вимогам. Він має понад 70 попередньо визначених налаштувань політики та категорій ризику. Їх можна вмикати або вимикати.

Інтерфейс SecureTrust DLP наведено на рис. 4.5.

SecureTrust може аналізувати всі веб-комунікації та вкладені файли на предмет порушень політики компанії, відповідності та прийнятного використання.

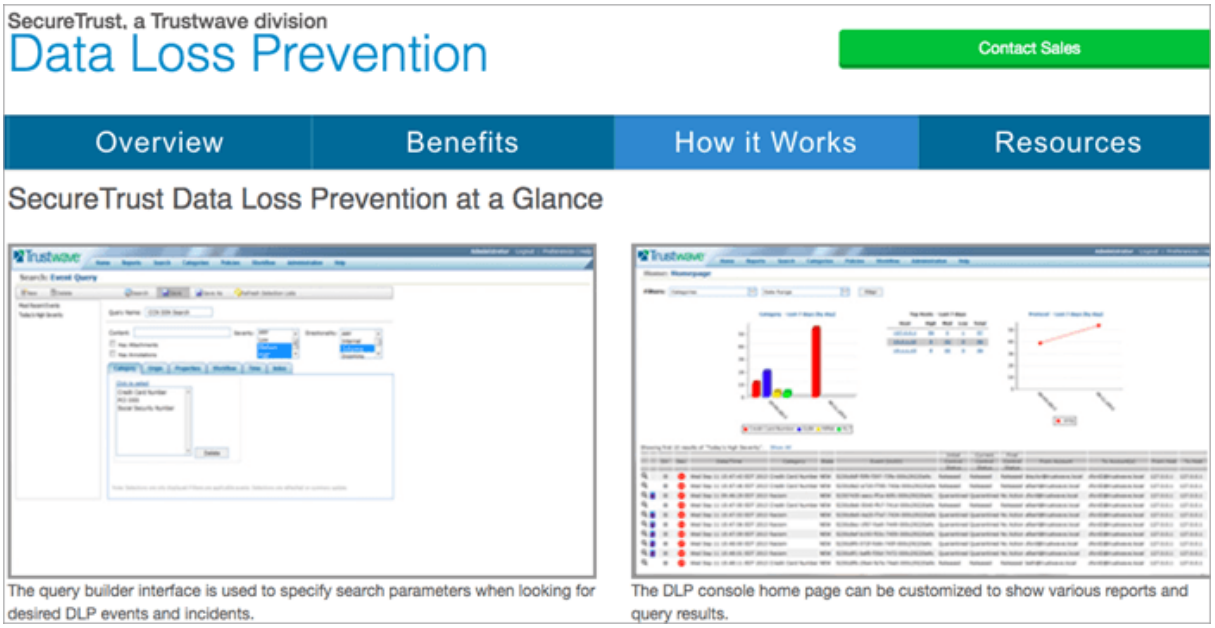

Рисунок 4.5 – Інтерфейс SecureTrust DLP

Основні характеристики SecureTrust DLP:

- функції автоматичного блокування HTTP, HTTPS і FTP-трафіку, який порушує політику відповідності;

- пропонує автоматичне шифрування, блокування, карантин або самовідповідність, якщо повідомлення електронної пошти та вкладення будуть визначені як порушення відповідності [12];

- інтелектуальний механізм керування вмістом, який допоможе командам безпеки виявляти конфіденційні дані, це дозволяє групам безпеки зосередитися на своїх ініціативах щодо конкретних користувачів і систем і впровадити правильні заходи;

- надає функції розширеного контролю вмісту, управління розслідуваннями та відповідності ідентифікаційних даних у реальному часі.

SecureTrust надає повну видимість усіх зовнішніх атак та інсайдерських ризиків. Крім того, він має приладову панель, яка легко налаштовується.

5 АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

5.1 Порівняльний аналіз програмного забезпечення DPL

У ході дослідження було проаналізовано 10 програмних засобів, з яких було обрано п’ять, які мають найкращі показники та характеристики для компаній: Endpoint Protector by CoSoSys, Symantec DLP, McAfee DLP, Forcepoint DLP, SecureTrust Data Loss Prevention (табл. 5.1). Порівняння цих п’яти програмних продуктів виконано за такими показниками: інструмент, тип компаній, платформи та розгортання.

Результати порівняльного аналізу представлені в табл. 3.1.

Таблиця 5.1 – Порівняння програмного забезпечення DPL

Програмне забезпечення DLP	Інструмент	Тип компаній	Платформи	Розгортання
1	2	3	4	5
Endpoint Protector by CoSoSys	Відкриття, відстеження та захист конфіденційних дані	Середні та корпоративні клієнти	Windows, Mac, Linux, принтери та тонкі клієнти	Віртуальний пристрій, хмарні послуги, розміщені в хмарі
Symantec DLP	Зменшення ризиків порушення даних і дотримання вимог	Підприємства	Windows, Mac, Linux	Хмарний і локальний
McAfee DLP	Захист від втрати даних	Малий і великий бізнес	Windows, Mac, Linux	Хмарний і локальний

Продовження табл.5.1.

1	2	3	4	5
Forcepoint DLP	Дані контролю-ються за допомогою єдиної політики	Малий і великий бізнес, агентства та підприємства	Windows і веб-додаток	Хмарна основа
SecureTrust Data Loss Prevention	Знаходження, відстеження та захист даних у всіх станах: Data At Rest, Data In Motion та Data In Use	Бізнес усіх галузей	Windows, Mac, Linux	Хмарний і локальний

5.2 Оцінка програмних засобів запобігання витоку інформації

В ході дослідження було проаналізовано 5 програмних засобів: Endpoint Protector by CoSoSys, Symantec DLP, McAfee DLP, Forcepoint DLP, SecureTrust Data Loss Prevention, які мають більш обширні відомості. Аналіз було проведено за такими показниками: платформи, розгортання, безкоштовний пробний період та інтеграції.

Під платформою розуміється цифрова платформа або обчислювальна платформа – зазвичай відноситься тільки до операційної системи та комп'ютерного обладнання. Платформа відповідає набору стандартів, які дозволяють розробникам програмного забезпечення розробляти програмні додатки для платформи. Ці ж стандарти дозволяють власникам і менеджерам купувати відповідні програми та обладнання [14]. Цей параметр оцінюється як 0,1 за кожну платформу, яка застосовується для того чи іншого програмного засобу.

Під розгортанням розуміється процес запуску програми на сервері або на

пристрої. Розгортання програмного забезпечення включає всі кроки, процеси та дії, які необхідні для того, щоб зробити систему програмного забезпечення чи оновлення доступними для передбачених користувачів [15]. Цей параметр оцінюється як 0,15 за кожен тип розгортання, що застосовується для того чи іншого програмного засобу.

Під безкоштовним пробнимий періодом розуміється модель придбання, коли продукт або послуга пропонується клієнтам протягом обмеженого періоду часу, безкоштовно, щоб вони могли дізнатися про продукт і дізнатися цінність, перш ніж фактично платити за нього [16]. Цей параметр оцінюється як 0,1 якщо доступна дана послуга або 0 якщо ні.

Під інтеграцією розуміється процес об’єднання різних типів програмних підсистем для створення єдиної системи [17]. Цей параметр оцінюється як 0,15 за кожен тип інтеграції, що застосовується для того чи іншого програмного засобу.

Результати аналізу оцінки програмних засобів запобігання витоку інформації представлені в табл. 5.2.

Таблиця 5.2 – Аналіз програмних засобів запобігання витоку інформації

Фактор	Класи-фікатор	Коефіцієнт	Назва програмного засобу				
			Endpoint Protector by CoSoSys	Symantec DLP	McAfee DLP	Forcepoint DLP	SecureTrust DLP
1	2	3	4	5	6	7	8
Плат-форми	Windows	0,1	+	+	+	+	+
	Mac		+	+	+		+
	Linux		+	+	+		+
	Принтер		+				
	Тонкий клієнт		+				
	Web-додатки					+	
Результат			0,5	0,3	0,3	0,2	0,3

Продовження табл. 5.2.

1	2	3	4	5	6	7	8
Розгор-тання	Віртуа-льний пристрій	0,15	+				
	Розмі-щення в хмарі		+				
	Хмарні послуги		+				
	Хмарна основа					+	
	Хмарний і локаль-ний			+	+		+
Результат			0,45	0,15	0,15	0,15	0,15
Безкош-товний пробний період	Так	0,05	+			+	
	Ні			+	+		+
Результат			0,05	0	0	0,05	0
Інтегра-ція	Мережа	0,1	+	+	+	+	+
	Сховище		+	+	+	+	+
	Хмара		+	+	+	+	+
	Кінцева точка		+	+	+	+	+
Результат			0,4	0,4	0,4	0,4	0,4
Загальний результат			1,4	0,85	0,85	0,8	0,85

За результатами оцінки програмних засобів для запобігання витоку інформації було встановлено, що найбільш ефективним є програмний продукт Endpoint Protector by CoSoSys. За результатами аналізу було побудовано діаграму оцінок програмних засобів (рис. 5.1).

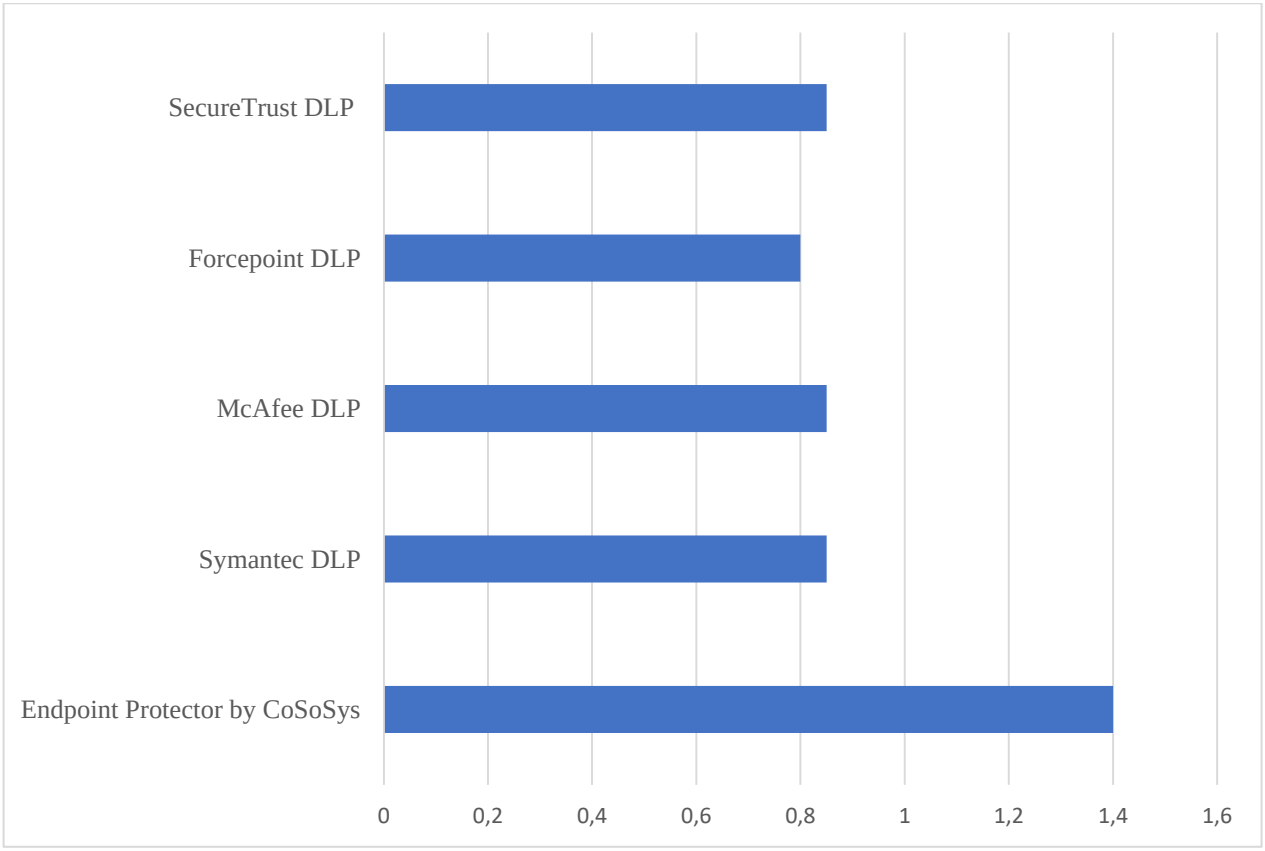

Рисунок 5.1 – Оцінка програмних засобів

ВИСНОВКИ

На даний момент втрата даних є серйозною проблемою для компаній будь-якого розміру – втрата файлів означає втрату часу та грошей на відновлення бізнесу або відновлення інформації, яка є важливою для бізнесу. Деякі втрачені дані можна відновити, але цей процес вимагає допомоги IT-фахівців і коштує часу та ресурсів, які бізнес може використовувати в інших цілях. В інших випадках втрачені файли та інформацію неможливо відновити, що робить запобігання втрат даних ще важливішим. Втрата даних є серйозною проблемою, яка порушує повсякденне функціонування будь-якої інформаційної сфери.

В роботі було розглянуто ряд питань, що стосуються сучасних технологій захисту інформації, та виконано аналіз програмних засобів для запобігання витоку інформації.

В першому розділі кваліфікаційної роботи проаналізовано актуальність питань захисту інформації у зв’язку зі стримким розвиткой інфокомунікацій в Україні, розглянуто основні причини для запобігання втрат даних та досліджено технології захисту інформації.

У другому розділі виконано огляд технології запобігання витоку даних, розглянуто основні функції систем захисту від витоків, а також переваги та недоліки DLP-систем.

Третій розділ присвячено захисту від витоку інформації протягом усього її життєвого циклу, а саме особливові захисту інформації в трьох станах Data at Motion, Data at Rest та Data in Use.

В четвертому розділі досліджено програмне забезпечення для запобігання втрат даних провідних постачальників на ринку, проаналізовано особливості та можливості цих програмних продуктів. Особливо детально було описано 5 програмних засобів: Endpoint Protector by CoSoSys, Symantec DLP, McAfee DLP, Forcepoint DLP та SecureTrust Data Loss Prevention.

У п’ятому розділі виконано порівняльний аналіз програмного забезпечення DPL за такими показниками: інструмент, тип компаній, платформи та розгортання. Виконано розрахунок оцінок для цих програмних засобів запобігання витоку інформації за такими показниками: платформи, розгортання, безкоштовний пробний період та інтеграції та порівняльний аналіз

за цими оцінками. За результатами оцінок програмних засобів для запобігання витоку інформації було встановлено, що найбільш ефективним є програмний продукт Endpoint Protector by CoSoSys.

В роботі підкреслено важливість захисту інформації оскільки відбувається стрімке зростання інформації, і тому підприємствам стає важко відстежувати, захищати та керувати конфіденційними даними в межах корпоративних кордонів. Рішення DLP допомагають компаніям запобігати витоку інформації та реагувати на інциденти.

Результати роботи було апробовано на дев’ятій міжнародній науково-технічній конференції «Проблеми інформатизації» та опубліковано тези доповіді [18] за тематикою кваліфікаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Bader S. What Is Data Loss Prevention and How Does It Work? [Електронний ресурс] / Sarah Bader // Rewind. – 2022. – Режим доступу до ресурсу: https://rewind.com/blog/data-loss-prevention/.

2. Reasons Why Your Business Needs (DLP) Data Loss Prevention [Електронний ресурс] // uniserve. – 2022. – Режим доступу до ресурсу: https://uniserveit.com/blog/reasons-why-your-business-needs-dlp-data-loss-prevention.

3. Tahboub R. Data Leakage/Loss Prevention Systems (DLP) [Електронний ресурс] / R. Tahboub, Y. Saleh // NNGT Journal: International Journal of Information Systems. – 2014. – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.4555&rep=rep1&type=pdf.

4. How Antivirus Works? [Електронний ресурс] // COMODO CYBERSECURITY. – 2020. – Режим доступу до ресурсу: https://antivirus.comodo.com/how-antivirus-software-works.php.

5. Petters J. What is SIEM? A Beginner's Guide [Електронний ресурс] / Jeff Petters // VARONIS. – 2020. – Режим доступу до ресурсу: https://www.varonis.com/blog/what-is-siem/.

6. An Overview of Firewalls [Електронний ресурс] // Atlantic Data Forensics. – 2018. – Режим доступу до ресурсу: https://www.atlanticdf.com/blog/2018/09/10/an-overview-of-firewalls/.

7. Data loss prevention definition [Електронний ресурс] // Druva. – 2020. – Режим доступу до ресурсу: https://www.druva.com/glossary/what-is-data-loss-prevention-definition-and-related-faqs/.

8. Гержан С. Г. Предотвращение утечки данных с помощью DLP-систем [Електронний ресурс] / С. Г. Гержан, Е. А. Масальская. – 2019. – Режим доступу до ресурсу: http://ir.nmu.org.ua/jspui/bitstream/123456789/148756/1/masalska_gerjan.pdf.

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

10. Security Guide [Електронний ресурс] // Fedora. – 2020. – Режим доступу до ресурсу: https://jfearn.fedorapeople.org/fdocs/en-US/Fedora/20/html/Security_Guide/Security_Guide-Encryption-Data_in_Motion.html.

11. Protecting the three states of data [Електронний ресурс] // Sealpath. – 2020. – Режим доступу до ресурсу: https://www.sealpath.com/blog/protecting-the-three-states-of-data/.

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

13. 11 BEST Data Loss Prevention Software DLP Solutions In 2022 [Електронний ресурс] // Software Testing Help. – 2022. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/data-loss-prevention-software/.

14. Platform [Електронний ресурс] // Techopedia. – 2020. – Режим доступу до ресурсу: https://www.techopedia.com/definition/3411/platform-computing#techopedia-explains-platform.

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

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

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

18. Аналіз технологій запобігання витоку інформації / С. Є. Пестєрєва, Д. В. Чеботарьова // Тези доповідей дев'ятої міжнародної науково-технічної конференції «Проблеми інформатизації», 18 – 19 листопада 2021 р., Черкаси – Баку – Бельсько-Бяла – Харків. – 2021. – Том 1. – С. 67.