Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Засоби захисту від витоку конфіденційної інформації підприємства на основі технології DLP»

Виконавець: студентка IV курсу, групи КБ-43

Поліна БОНДАРЕНКО
(підпис) (ім'я прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Яніна ШЕСТАК
Нормоконтроль		Іван БІЛОКОНЬ

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

Студентці **КБ-43** **Бондаренко Поліні Віталіївні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби захисту від витоку конфіденційної інформації підприємства на основі технології DLP

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи попередження витоку конфіденційної інформації на підприємстві

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з функціями та принципами роботи технологій DLP та з DLP-рішеннями постачальників

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо підвищення ефективності попередження витоку конфіденційної інформації підприємства використовуючи технології DLP.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Поліна БОНДАРЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 20.01.2025	*виконано*
2	Аналіз літератури	21.01.2025 – 06.03.2025	*виконано*
3	Обґрунтування вибору рішення	07.03.2025 – 10.03.2025	*виконано*
4	Дослідження методів захисту інформації	11.03.2025 – 15.04.2025	*виконано*
5	Дослідження принципу роботи DLP-систем	16.04.2025 – 06.05.2025	*виконано*
6	Дослідження існуючих DLP-рішень	07.05.2025 – 19.05.2025	*виконано*
7	Розробка рекомендацій щодо підвищення ефективності роботи DLP-систем	20.05.2025 – 28.05.2025	*виконано*
8	Оформлення пояснювальної записки	28.05.2025 – 28.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	29.05.2025 – 13.06.2025	*виконано*

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Поліна БОНДАРЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 59 сторінки основного тексту, 3 рисунки та 3 таблиці. Список використаних джерел містить 31 найменування і займає 4 сторінки.

Метою роботи є підвищення ефективності системи захисту конфіденційної інформації підприємства використовуючи технологію DLP.

Для досягнення зазначеної мети поставлено наступні завдання:

- проаналізувати поняття конфіденційної інформації та основні загрози її витоку;
- дослідити методи захисту інформації, зокрема DLP-технологію;
- визначити переваги та недоліки впровадження DLP на підприємстві;
- провести порівняльний аналіз популярних DLP-рішень;
- запропонувати удосконалення системи захисту конфіденційної інформації із використанням DLP.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки на підприємстві.

Предметом дослідження є технологія Data Loss Prevention (DLP) як інструмент попередження витоку конфіденційної інформації.

Практичною цінністю отриманих результатів є рекомендації щодо підвищення ефективності попередження витоку конфіденційної інформації підприємства використовуючи технології DLP

Ключові слова: захист інформації, конфіденційна інформація, кібербезпека, канали витоку, загрози інформації, DLP-система, Data Loss Prevention, покращення ефективності.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DLP	–	Data Loss Prevention
КІ	–	Конфіденційна інформація
АС	–	Автоматизована система
ПЗ	–	Програмне забезпечення
СЗІ	–	Система захисту інформації
НСД	–	Несанкціонований доступ
ЗУ	–	Закон України
АТ	–	Акційне товариство

ВСТУП

На сьогоднішній день підприємства переходять у цифровий формат та щодня працюють з великою кількістю конфіденційної інформації. Це можуть бути персональні дані працівників, клієнтів, фінансова документація, комерційна таємниця, важливі для підприємства розробки та інше. Витік такої інформації призводить до фінансових збитків, втрати довіри клієнтів, партнерів, та репутації в цілому.

Сучасні системи безпеки в підприємствах мають працювати як на виявлення загроз, так і на активне попередження витоку інформації. Для цього існує DLP технологія, Data Loss Prevention − запобігання витоку інформації, яка дозволяє контролювати як переміщується інформація всередині підприємства та за його межами так і своєчасно виявляти підозрілі дії та блокувати потенційно небезпечну передачу даних.

Отже, *актуальність теми* зумовлена необхідністю підприємств захищати конфіденційні дані, тому *метою роботи* є підвищення ефективності системи захисту конфіденційної інформації підприємства з допомогою технологію DLP.

Для досягнення цієї мети роботи поставлені такі *завдання*:

- проаналізувати поняття конфіденційної інформації та основні загрози її витоку;
- дослідити методи захисту інформації, зокрема DLP-технологію;
- визначити переваги та недоліки впровадження DLP на підприємстві;
- провести порівняльний аналіз популярних DLP-рішень;
- запропонувати удосконалення системи захисту конфіденційної інформації із використанням DLP.

Результатом роботи є розроблені нами рекомендації для підвищення ефективності попередження витоку конфіденційної інформації підприємства використовуючи технологію DLP.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ, ЗАГРОЗИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

1.1. Поняття конфіденційної інформації

Згідно термінологічного навчального довідника, конфіденційність інформації - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею [1].

Конфіденційна інформація, незалежно від сфери її застосування, має важливе значення для її власника. Її цінність визначається використанням у публічній сфері (наприклад, для державного управління) та приватній (для реалізації та захисту прав держави, громадян і організацій). Доступ до такої інформації третіх осіб може зашкодити як державним, так і приватним інтересам. Класифікація конфіденційних відомостей дозволить систематизувати дані про інформацію з обмеженим доступом і визначити її особливості, що сприятиме кращому розумінню її сутності.

Незважаючи на існування численних наукових розробок і досліджень, єдиного універсального підходу до класифікації конфіденційної інформації досі не вироблено. Різні джерела пропонують власні варіанти класифікації, які відрізняються критеріями, рівнями захисту та сферами застосування [2].

1.2. Основні загрози витоку інформації

Загроза − можлива небезпека; будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі [1].

Інформаційні загрози аналізуються з огляду на їхній потенційно негативний вплив на ключові аспекти інформаційної безпеки та ймовірність їх підриву. У сфері автоматизованих систем (АС) традиційно класифікують такі види загроз:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в наданні сервісу (обслуговуванні);
- порушення спостережуваності або керованості.

Таким чином, під загрозою розуміють будь-яку потенційно реалізовану дію, здатну завдати шкоди інформаційним активам через компрометацію однієї або декількох їхніх характеристик.

Особливу увагу в даному контексті приділяється компрометації конфіденційності.

Сучасний аналіз методів захисту даних свідчить, що існує два первинні механізми порушення конфіденційності:

- втрата контролю над системою захисту інформації (СЗІ).
- виникнення каналів витоку інформації.

Інші сценарії втрати конфіденційності, по суті, є похідними від цих двох категорій.

У разі несправності або неефективної роботи СЗІ створюються умови для реалізації несанкціонованого доступу (НСД) до захищених відомостей [3].

Витік інформації − несанкціонований процес перенесення інформації від джерела до зловмисника. Витік інформації є можливим шляхом її розголошення людьми, втрати ними носіїв з інформацією, перенесення інформації за допомогою випромінювання, потоків елементарних часток, речовин в газоподібному, рідкому або твердому стані. Витік інформації у порівнянні з утратою (викраденням) матеріальних об'єктів має ряд особливостей, які необхідно враховувати при організації захисту інформації: витік інформації може здійснюватися тільки при попаданні її до зацікавленого в ній несанкціонованого одержувача (зловмисника); при витоку інформації здійснюється її тиражування, яке не змінює харак-

теристики носія інформації; ціна інформації при її витоку зменшується за рахунок тиражування; факт витоку інформації, як правило, виявляється через деякий час, за наслідками витоку, коли заходи забезпечення її безпеки можуть виявитися неефективними. Витік інформації здійснюється каналами витоку. Просочування в засоби масової інформації відомостей із закритих або малодоступних джерел. Ці відомості можуть або слугувати на благо суспільним інтересам, або стати засобом маніпулювання суспільною думкою [1].

Загрози можуть реалізуватися внаслідок багатьох причин, серед яких:

- кількісна недостатність – фізична нестача компонентів АС для протидії можливим порушенням безпеки інформації;
- якісна недостатність – недосконалість конструкції або організації компонентів АС, внаслідок чого не забезпечується протидія можливим порушенням безпеки інформації;
- відмови елементів АС – порушення працездатності елементів, яке призводить до неможливості виконання ними своїх функцій;
- збої елементів АС – тимчасове порушення працездатності елементів, яке призводить до неправильного виконання ними в деякий момент часу своїх функцій;
- помилки елементів АС – неправильне (одноразове або систематичне) виконання елементами своїх функцій внаслідок специфічного (постійного або тимчасового) їх стану;
- стихійні лиха – явища, що виникають випадково, не контролюються і призводять до фізичних зруйнувань;
- зловмисні дії – дії людей, що спеціально спрямовані на порушення безпеки інформації;
- побічні явища – явища, що супутні виконанню елементом АС своїх функцій.

Джерелами наведених причин порушення безпеки можуть бути:

- особи, що мають будь-яке відношення до функціонування АС;
- технічні засоби;

- моделі, алгоритми, програмне забезпечення (ПЗ);
- технологія функціонування – сукупність засобів, прийомів, правил, заходів і погоджень, що використовуються в процесі обробки інформації;
- зовнішнє середовище – сукупність елементів, що не входять до складу АС, але можуть впливати на захищеність інформації в АС [3].

1.3. Методи та технології захисту інформації

Далі ми розглянемо як саме ми можемо захистити інформацію від витоку. Існують інженерно-технічні та організаційно-правові засоби захисту, розглянемо перші.

Засоби інженерно-технічного захисту класифікуються за функціональним призначенням на:

- фізичні засоби – це різні пристрої та конструкції, які запобігають несанкціонованому проникненню на об’єкти захисту або доступ до носіїв конфіденційної інформації. Вони також захищають персонал, матеріальні активи, фінансові ресурси та інформацію від протиправних дій.
- апаратні засоби – це технічні пристрої, механізми та інші рішення, призначені для захисту даних. На підприємствах використовується різноманітне обладнання – від звичайних телефонів до складних автоматизованих систем, які підтримують виробничі процеси. Головна функція таких засобів – запобігання витоку інформації, її розголошенню та несанкціонованому доступу через технічні канали.
- програмні засоби – це спеціалізовані програми та програмні комплекси, які забезпечують захист даних у інформаційних системах і при їх обробці (збиранні, накопиченні, зберіганні, передачі тощо).
- криптографічні засоби – математичні та алгоритмічні методи захисту інформації, що передається через мережі зв’язку або зберігається на комп’ютерах. Вони передбачають використання різних технік шифрування для забезпечення конфіденційності даних.

Фізичні засоби є першою лінією оборони в будь-якій системі захисту інформації. Їх завдання створювати перешкоди для фізичного доступу до місць, де зберігається, обробляється або передається інформація. До таких засобів належать різноманітні механічні, електронні та електромеханічні пристрої, які встановлюються для запобігання несанкціонованому проникненню на об'єкти захисту. Це можуть бути огорожі, сигналізація, системи відеоспостереження, спеціальні двері, замки, решітки на вікнах, системи контролю доступу, охоронне телебачення, пожежна сигналізація, а також фізичні бар’єри, які забезпечують запобігання прямому впливу на інформаційні ресурси.

Такі засоби не тільки ускладнюють несанкціонований доступ, але й виконують функції виявлення вторгнень та нейтралізації загроз. Наприклад, відеоспостереження може зафіксувати спробу проникнення, а системи охоронної сигналізації автоматично реагують на порушення й інформують службу безпеки. Таким чином, фізичний захист забезпечує базовий рівень інформаційної безпеки, що є критично важливим у поєднанні з іншими типами захисту.

Апаратні засоби це спеціалізовані технічні пристрої, які забезпечують захист інформації на рівні електроніки та обладнання. Вони використовуються для запобігання витоку даних, протидії несанкціонованому доступу та виявлення каналів перехоплення. Сюди входять як прості технічні рішення, наприклад, контролери доступу, засоби блокування портів, засоби ізоляції комунікаційних каналів, так і складні системи апаратного аналізу каналів витоку інформації.

Особливістю апаратних засобів є те, що вони діють на базовому рівні роботи обчислювальних машин та периферії. Вони можуть аналізувати й обмежувати доступ до внутрішніх компонентів комп’ютера, контролювати звернення до носіїв інформації, а також захищати важливі області пам’яті від несанкціонованої модифікації. Такі засоби особливо ефективні в середовищах, де потрібен постійний моніторинг і реакція на зміну технічних умов експлуатації.

Крім того, апаратні методи є важливими у боротьбі з промисловим шпигунством, адже дають змогу виявити спеціальні пристрої, призначені для несан-

кціонованого збору даних. Завдяки своїй незалежності від програмного забезпечення, апаратні засоби часто залишаються ефективними навіть у разі комп'ютерних збоїв або атак.

Програмні засоби є найбільш гнучкими і поширеними елементами сучасних систем захисту інформації. Вони охоплюють широкий спектр програмного забезпечення, яке забезпечує безпечну роботу обчислювальних систем. Такі засоби виконують ідентифікацію користувачів, контроль за їхніми діями, розмежування прав доступу, ведення журналів подій, захист від вірусів, шкідливого коду, а також реалізують шифрування каналів зв'язку.

Важливою функцією програмного захисту є запобігання несанкціонованому доступу до ресурсів системи. Це досягається через введення паролів, автентифікацію, а також використання систем багатоетапної перевірки доступу. Програми можуть контролювати, які користувачі мають доступ до яких файлів, коли і які дії вони виконують. Якщо порушення фіксуються, система може автоматично обмежити доступ або повідомити адміністратора.

Також важливим аспектом є боротьба з комп'ютерними вірусами та шкідливим програмним забезпеченням. Сучасні антивірусні системи здатні виявляти тисячі типів загроз, а також оновлювати бази сигнатур, щоб залишатися ефективними в нових умовах. Деякі програмні продукти навіть можуть знищити віруси або відновити пошкоджені файли.

Загалом, програмні засоби працюють у тісному зв'язку з апаратними та організаційними заходами, створюючи багаторівневий захист, який дозволяє ефективно протидіяти більшості сучасних кіберзагроз.

Криптографія – це математична основа захисту інформації, яка дозволяє перетворити її в таку форму, що є недоступною для розуміння сторонніми особами. Вона забезпечує конфіденційність, цілісність та автентичність даних у процесі їх зберігання або передавання.

Основним інструментом криптографії є шифрування, перетворення повідомлення у вигляд, що не може бути зрозумілим без спеціального ключа. Сучасні

системи використовують як симетричні алгоритми шифрування (один і той самий ключ для шифрування і дешифрування), так і асиметричні (використання відкритого та закритого ключів, наприклад, у системах електронного підпису чи HTTPS).

Криптографічні засоби стали особливо важливими з поширенням Інтернету та мобільного зв'язку. Вони гарантують, що навіть у разі перехоплення повідомлення сторонні не зможуть його прочитати або змінити. Це особливо критично для фінансових установ, державних органів та комерційних структур, де витік інформації може призвести до суттєвих збитків.

Криптографічні методи вважаються одними з найнадійніших у сфері інформаційної безпеки. Якщо алгоритм і ключі побудовані за сучасними стандартами, їх злам є надзвичайно складним і дорогим завданням, часто навіть неможливим у прийнятний час. Проте варто пам'ятати, що захист залежить також від правильного управління ключами, їх зберігання та оновлення [4].

Таким чином, захист інформації реалізується за допомогою комплексного застосування фізичних, апаратних, програмних і криптографічних засобів, що разом забезпечують безпеку даних від витоку і несанкціонованого доступу.

1.4. Нормативна база КІ

Захист інформації забезпечується не тільки з допомогою фізичних, апаратних, програмних і криптографічних засобів, а також використанням нормативно-правової бази на державному рівні:

Конституція України стаття 32 – не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [5].

ЗУ «Про інформацію» – регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [6].

ЗУ «Про захист персональних даних» – регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних [7].

ЗУ «Про доступ до публічної інформації» – визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [8].

ЗУ «Про державну таємницю» – регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [9].

ЗУ «Про захист інформації в інформаційно-комунікаційних системах» - регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [10].

ЗУ «Про електронну ідентифікацію та електронні довірчі послуги» – визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов’язки суб’єктів відносин у сферах електронної ідентифікації та електронних довірчих послуг, порядок здійснення державного контролю за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг [11].

ЗУ «Про основні засади забезпечення кібербезпеки України» – визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [12].

«Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» Кабінет Міністрів України Постанова від 29 березня 2006 р. № 373 – ці Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [13].

Кодекс України про адміністративні правопорушення – завданням Кодексу України про адміністративні правопорушення є охорона прав і свобод громадян, власності, конституційного ладу України, прав і законних інтересів підприємств, установ і організацій, встановленого правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян у дусі точного і неухильного додержання Конституції і законів України, поваги до прав, честі і гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов'язків, відповідальності перед суспільством [14].

Глава 15 − Адміністративні правопорушення, що посягають на встановлений порядок управління, стаття 188-39 – порушення законодавства у сфері захисту персональних даних [14].

Кримінальний кодекс України – має своїм завданням правове забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від кримінально-протиправних посягань, забезпечення миру і безпеки людства, а також запобігання кримінальним правопорушенням [15].

Розділ XVI Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [15].

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги – стандарт, що встановлює вимоги до системи керування інформаційною безпекою в організаціях [16].

Указ Президента України *Положення про технічний захист інформації в Україні* – визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства [17].

НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці [18].

Також створюються методичні рекомендації, наприклад *«Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами»*, вони не є нормативно-правовими актами, несуть рекомендаційний характер і є добровільними для використання [19].

1.5. DLP-система для захисту конфіденційних даних

Серед різноманітних методів захисту ми детально будемо розглядати Data Loss Prevention системи. DLP-система поєднує в собі активні та пасивні засоби захисту інформації та переважно є програмним рішенням. Вона створена з метою виявлення, моніторингу та запобігання несанкціонованому розповсюдженню конфіденційної інформації як всередині організації, так і за її межами.

Застосування DLP-систем особливо важливе для захисту чутливої інформації, такої як персональні дані клієнтів, комерційна таємниця, фінансові документи чи інтелектуальна власність. Впровадження таких систем допомагає мінімізувати ризики витоків, які можуть мати серйозні фінансові, репутаційні та правові наслідки для організації.

У наступному розділі буде детально розглянуто, що саме являє собою DLP, які основні функції та компоненти входять до складу таких систем.

Висновки до розділу 1

1. Конфіденційна інформація − це інформація, доступ до якої обмежено, і яка має цінність для держави, юридичних чи фізичних осіб. Її розголошення може завдати шкоди публічним або приватним інтересам. Загальної класифікації немає через те, що існують різні критерії, рівні захисту та сфери її застосування.

2. Загроза − це потенційно небезпечна подія або дія, яка може порушити безпеку інформації в системі. Витік − це несанкціоноване перенесення інформації до зловмисника через різні канали (технічні або людські).

Найпоширенішими шляхами порушення конфіденційності є втрата контролю над системою захисту інформації та канали витоку інформації.

Витік інформації може здійснюватися через: помилки або збої в роботі елементів АС, фізичні пошкодження, недосконале або застаріле програмне забезпечення, людський фактор (ненавмисні чи навмисні дії), технічні канали (наприклад, електромагнітне випромінювання, втрати носіїв тощо).

Причинами реалізації загроз можуть бути: кількісна та якісна недостатність систем безпеки, відмови, збої чи помилки елементів системи, стихійні лиха, зловмисні дії осіб, вплив зовнішнього середовища.

Джерелами загроз можуть бути: персонал, який працює з АС, технічні засоби й ПЗ, технології обробки інформації, зовнішні фактори (природні чи штучні).

3. Існують два основні види засобів захисту інформації: інженерно-технічні та організаційно-правові. Інженерно-технічні засоби поділяються на: фізичні, апаратні, програмні та криптографічні.

Фізичні засоби − пристрої та споруди, які перешкоджають фізичному доступу зловмисників до об’єктів та носіїв інформації. Вони охороняють територію, приміщення, обладнання, а також контролюють доступ.

Апаратні засоби − технічні пристрої, які забезпечують захист інформації від розголошення, витоку і несанкціонованого доступу, включаючи виявлення і локалізацію каналів витоку, боротьбу з промисловим шпигунством.

Програмні засоби − спеціальне програмне забезпечення і системи захисту, які працюють на комп’ютерах і в інформаційних системах, захищаючи від несанкціонованого доступу і інших загроз. Вони класифікуються на засоби власного захисту, активного і пасивного захисту тощо.

Криптографічні засоби − математичні та алгоритмічні методи шифрування, які забезпечують безпеку передачі, зберігання і обробки інформації.

Для захисту інформації використовується комплексний підхід з усіма засобами.

4. Data Loss Prevention – це переважно програмне рішення, яке поєднує активні та пасивні засоби захисту інформації. Вона призначена для виявлення, моніторингу та запобігання несанкціонованому розповсюдженню конфіденційних даних всередині організації і за її межами. Особливо важлива для захисту чутливої інформації - персональних даних, комерційної таємниці, фінансових документів та інтелектуальної власності. Впровадження DLP-систем допомагає зменшити ризики витоків, що можуть призвести до фінансових, репутаційних і правових втрат.

РОЗДІЛ 2
ВІДОМОСТІ ПРО ТЕХНОЛОГІЮ DLP ТА АНАЛІЗ DLP-СИСТЕМ

2.1. Загальні відомості про DLP-системи

В цьому пункті ми детально розглянемо, що таке DLP-система, її основне призначення, з яких компонентів складається, де знаходиться, виділимо ключові функції, які вона виконує, та розглянемо за якими принципами працює DLP.

Абревіатура DLP означає Data Loss Prevention або «запобігання втраті даних». Це сукупність методів та інструментів, які застосовуються мережевими адміністраторами для захисту конфіденційної інформації від несанкціонованого доступу, викрадення чи втрати. Такий підхід спрямований на запобігання витоку критично важливих даних за межі корпоративної мережі. Оскільки користувачі можуть як ненавмисно, так і навмисно передавати чутливу інформацію стороннім, це становить потенційну загрозу для безпеки організації [20, 21].

Запобігання втраті даних (DLP) виявляє, контролює та захищає передачу даних за допомогою глибокої перевірки вмісту та аналізу параметрів транзакцій (таких як джерело, пункт призначення, об'єкт даних та протокол) за допомогою централізованої системи управління. Тобто, DLP виявляє та запобігає несанкціонованій передачі конфіденційної інформації [22].

Ця технологія забезпечення безпеки призначена для захисту конфіденційної інформації в автоматичному та непомітному для користувача режимі. DLP-система використовує спеціально налаштовані політики, які дозволяють контролювати обіг даних, гарантуючи, що критично важлива інформація не зберігається, не передається і не відкривається у невідповідних місцях. При цьому користувачі можуть продовжувати працювати з необхідними їм сервісами та інструментами без обмежень, якщо це не порушує політик безпеки. На відміну від жорстких методів контролю на основі білих і чорних списків, DLP-технологія вибірково блокує лише ті дії, які стосуються конфіденційних даних, наприклад,

надсилання електронного листа дозволено, якщо він не містить чутливої інформації або не прямує за межі корпоративного середовища [23, 24].

Прикладом потенційного порушення безпеки є завантаження конфіденційних файлів до сторонніх комерційних хмарних сервісів, наприклад, Dropbox, що може призвести до витоку інформації. DLP-системи дозволяють виявляти, класифікувати та контролювати такі дії, захищаючи чутливі дані незалежно від їх типу, чи то внутрішньо робоча інформація, комерційна таємниця, чи персональні дані, які підлягають правовому захисту. Завдяки цьому забезпечується цілісність і безпечне використання інформації в межах організації [20].

Основна мета DLP-систем полягає в тому, щоб запобігти випадковому або навмисному витоку конфіденційної інформації з боку співробітників, які мають до неї доступ у межах своїх службових повноважень [20, 25]. У сучасному корпоративному середовищі саме внутрішні користувачі можуть становити серйозну загрозу, особливо коли мова йде про передачу важливої інформації поза межі організації. DLP-системи зосереджені на захисті таких каналів, як електронна пошта, веб-трафік (зокрема HTTP-запити), тіньові копії файлів, дані, що передаються на друк, та інші подібні потоки [20, 26].

Завдяки гнучким налаштуванням, DLP-системи здатні забезпечувати три ключові функції, що дозволяють ідентифікувати спроби витоку інформації, захищати дані та оперативно реагувати на загрози. У режимі моніторингу система лише фіксує підозрілу активність без блокування дій, що особливо корисно на етапі впровадження політик або для оцінки рівня ризиків. У режимі попередження користувач отримує сповіщення про можливе порушення правил обігу даних, що сприяє формуванню культури відповідального поводження з конфіденційною інформацією. У найсуворішому режимі, блокуванні, система повністю припиняє виконання небажаної дії, наприклад, забороняє надсилання електронного листа або збереження документа на зовнішній носій, якщо це порушує встановлені політики [20, 27].

Завдяки своїм можливостям DLP-системи формують надійний «цифровий периметр» навколо організації, контролюючи не лише вихідні, а іноді й вхідні

потоки інформації. Вони виступають важливим елементом в архітектурі інформаційної безпеки, допомагаючи знизити ризики витоку даних та підвищити загальний рівень захищеності бізнесу.

Також виділяють такі функції DLP-систем окрім загальних:

- контроль передачі даних по протоколу FTP;
- контроль HTTP трафіку;
- контроль безпровідних мереж;
- інтеграція з Proxy-серверами;
- контроль обміну повідомленнями через соціальні мережі;
- розгортання у віртуальному середовищі;
- сканування робочих станцій;
- контроль буферу обміну;
- контроль баз даних та мережевих сховищ;
- інтеграція з LDAP;
- інтеграція з системами документообігу [20].

Не існує єдиної думки щодо того, що саме включає в себе DLP-рішення. Деякі вважають, що до нього належать шифрування або контроль USB-портів, тоді як інші обмежують цей термін повноцінними продуктами. Securosis визначає DLP як продукти, які на основі централізованих політик ідентифікують, відстежують і захищають дані, що перебувають у стані спокою, передачі та використання, за допомогою глибокого аналізу вмісту. Отже, ключові характеристики DLP:

- глибокий аналіз вмісту;
- централізоване управління політиками;
- широке покриття вмісту на різних платформах і локаціях.

Іноді підприємства класифікують дані детальніше, ніж просто «публічні» та «все інше». DLP допомагає організаціям краще розуміти свої дані та підвищує їхню здатність класифікувати й управляти вмістом. Повноцінні (full-suite) рі-

шення забезпечують повне покриття вашої мережі, сховищ даних і кінцевих точок, навіть якщо не використовуються всі їхні можливості. Існують ще три альтернативні підходи:

● часткові DLP-рішення (Partial-suite DLP solutions) − це спеціалізовані інструменти DLP, які охоплюють два можливі канали (наприклад, мережу та сховища) та включають повний робочий процес (наприклад, управління інцидентами) і можливості аналізу вмісту;

● одноканальні DLP-рішення (Single-channel DLP solutions) охоплюють лише один канал, але все ще містять повний робочий процес DLP і можливості аналізу вмісту;

● функції DLP у складі інших продуктів (DLP features in other products) це компоненти, інтегровані в різноманітні продукти, які забезпечують часткове покриття та обмежені можливості аналізу вмісту, зазвичай без повноцінного робочого процесу DLP [28].

DLP-системи класифікуються за способом їх розгортання та взаємодії з об'єктами моніторингу. Вони поділяються на три основні типи: агентні (agent-based), безагентні (agentless) та гібридні (hybrid).

Агентні системи передбачають обов’язкове встановлення спеціального програмного забезпечення на кожен кінцевий пристрій, що забезпечує найглибший рівень контролю. Такий підхід дозволяє не лише виявляти порушення, але й відстежувати локальні дії користувачів, наприклад, спроби копіювання файлів на флеш-накопичувачі чи знімні диски, друк документів або використання буфера обміну. Ці системи особливо ефективні в організаціях з великою кількістю віддалених працівників або при необхідності контролю за діяльністю користувача незалежно від підключення до корпоративної мережі.

Безагентні DLP-системи не потребують встановлення програм на кінцеві пристрої. Вони діють шляхом аналізу трафіку в мережі, контролюючи, наприклад, пересилання електронної пошти, веб-запити або передачу файлів. Такий

підхід простіший у впровадженні та не потребує втручання в конфігурацію робочих місць, однак не дозволяє отримати повний контроль над локальною активністю користувача.

Гібридні рішення поєднують переваги обох підходів. Вони здатні як здійснювати глибокий аналіз на рівні кінцевого пристрою, так і моніторити трафік усередині мережі, забезпечуючи максимальну гнучкість і ефективність. Завдяки цьому гібридні DLP-системи здатні адаптуватися до різних умов використання, масштабуватися під потреби великого підприємства та забезпечувати всебічний захист інформації.

При виборі DLP-рішення однією з найважливіших характеристик, яку необхідно враховувати, є мережева архітектура організації. Саме вона визначає доцільність використання певного типу системи, її масштабованість, можливості інтеграції з іншими інструментами безпеки та рівень контролю, який можна реалізувати. Відповідно до цього, продукти класу, що розглядається, поділяються на дві великі групи: шлюзові (рис. 1.1) і хостові (рис. 1.2).

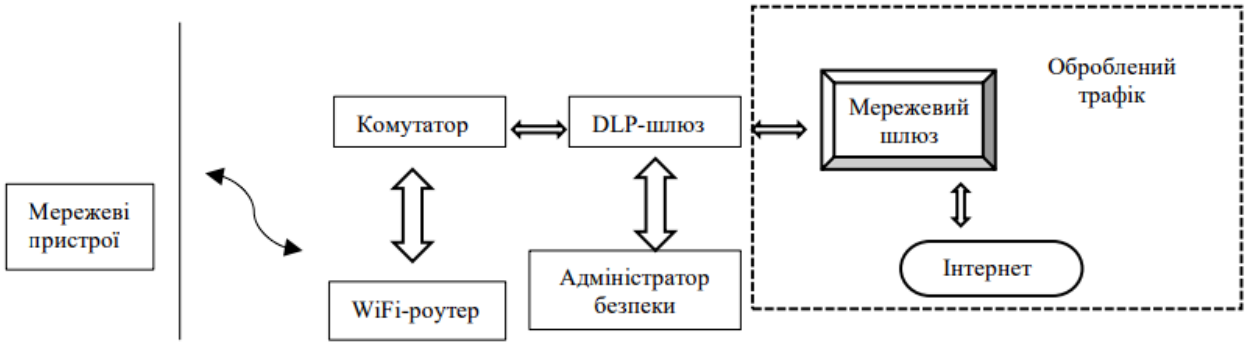

Рисунок 1.1 – Схема шлюзового DLP-рішення [20]

У першій групі використовується єдиний сервер, на який надсилається весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз займається його обробкою з метою виявлення можливих витоків конфіденційних даних.

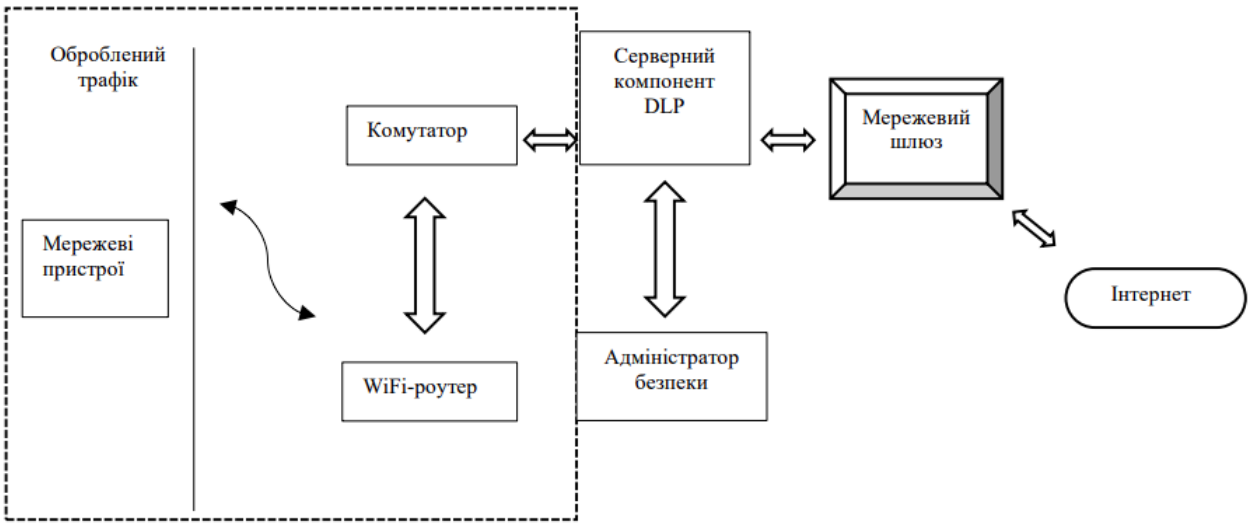

Рисунок 1.2 – Схема хостового DLP-рішення [20]

Другий варіант заснований на використанні спеціальних програм - агентів, які встановлюються на кінцевих вузлах мережі - робочих станціях, серверах додатків та ін. Останнім часом спостерігається стійкий перехід до універсалізації DLP-систем. На ринку залишилося мало або зовсім не залишилося рішень, які називаються чисто хостинговими або шлюзовими рішеннями [20].

У центрі будь-якої системи DLP лежать політики, набір правил, що визначає, яка інформація вважається чутливою, як вона повинна оброблятися, де може зберігатися і куди може передаватися. Без чітко визначених політик система DLP не змогла б розрізняти публічні дані від критично важливих, а отже, не мала б змоги ефективно захищати інформаційні активи організації. Політики можуть формуватися на основі внутрішніх вимог компанії, наприклад, специфіки бізнес-процесів, корпоративної етики або рівнів доступу, а також на базі зовнішніх нормативних стандартів, таких як PCI DSS, GDPR, HIPAA та інші галузеві або регіональні регуляції. Таким чином, DLP-система дозволяє адаптуватися як до внутрішніх, так і до зовнішніх вимог безпеки.

Створення політик одна з найважливіших і найскладніших стадій впровадження DLP, яка потребує участі не лише IT-фахівців, але й представників різних підрозділів компанії. Це командна робота, у межах якої потрібно проаналізувати

вже існуючі політики, зрозуміти, які типи даних є критичними, та спільно визначити підхід до їх класифікації, ідентифікації та захисту. Наприклад, фінансові звіти, медичні записи, код розробки, персональні дані клієнтів можуть мати різні рівні чутливості та вимагати різного рівня контролю.

Після погодження та формалізації політики вона перетворюється на набір технічних правил, які застосовуються всередині DLP-системи, визначаються ключові слова, шаблони, цифрові відбитки або інші критерії, за якими система виявлятиме й захищатиме визначений тип інформації. Наприклад, якщо політика компанії визначає, що джерельний код на Java є важливим активом і повинен зберігатися лише в корпоративному репозиторії та на робочих станціях розробників, то будь-яка спроба завантажити цей код в інше місце (наприклад, на зовнішній диск або в особисту хмару) розглядатиметься як порушення. DLP-система в такому випадку автоматично застосовує політику, блокує дію, надсилає повідомлення про інцидент або генерує звіт для адміністратора безпеки [23].

Інформаційні потоки, що підлягають контролю з боку DLP-систем, охоплюють значно ширший спектр, ніж просто інтернет-трафік. Під захистом опиняються всі можливі шляхи переміщення конфіденційних даних, включно з файлами, які копіюються на зовнішні носії, роздруковуються на принтерах, надсилаються через Bluetooth чи Wi-Fi або передаються за межі внутрішнього периметра інформаційної системи. DLP-системи працюють на рівні контролю трафіку, постійно аналізуючи його вміст. У разі виявлення конфіденційної інформації система миттєво активує захисні механізми, наприклад, блокує пересилання повідомлення, припиняє сеанс зв’язку або блокує запис на зовнішній носій.

Для ідентифікації чутливої інформації DLP використовує складні механізми аналізу, зокрема вміст документів і наявність характерних ознак, як-от службові печатки, спеціальні текстові мітки чи контрольні значення хеш-функцій. Це дозволяє точно визначити, чи містить передаваний документ конфіденційні відомості, незалежно від його формату або способу відправлення [20, 29, 30].

Методи виявлення витоків умовно поділяють на дві основні категорії: проактивні та реактивні.

Проактивні методи базуються на аналізі самого вмісту інформації. Наприклад, морфологічний аналіз дозволяє виявляти певні ключові слова або фрази, що зазвичай зустрічаються в конфіденційних документах. Це один із найпоширеніших способів виявлення витоку інформації, орієнтований на текст. Статистичний аналіз використовує ймовірнісні моделі, які дозволяють оцінити, наскільки той чи інший текст є подібним до відомих зразків конфіденційних даних. Цей метод вимагає попереднього навчання системи на прикладах документів, що підлягають захисту. Також широко застосовуються регулярні вирази − шаблони, що описують структуру чутливої інформації (наприклад, номери кредитних карт або паспортів), які система шукає у вхідних і вихідних даних [20, 31].

До реактивних методів належать цифрові відбитки та цифрові мітки. Цифровий відбиток − це унікальний набір характеристик документа, який дозволяє пізніше з високою точністю виявити навіть його часткове використання. Сучасні DLP-системи здатні розпізнавати як повні файли, так і їх фрагменти, та визначати ступінь схожості з оригіналом. Це дозволяє створювати гнучкі правила реагування залежно від рівня збігу. У свою чергу, цифрові мітки наносяться на документ спеціально, зазвичай у прихованій формі, й зчитуються лише за допомогою DLP-системи. Завдяки цьому можна не тільки визначити спробу витоку, а й контролювати можливі дії з документом: копіювання, надсилання, збереження тощо.

Таким чином, сучасні DLP-рішення забезпечують глибокий контентний аналіз та контроль, що дозволяє вчасно виявляти і блокувати потенційно небезпечні дії, пов’язані з витоком інформації, навіть до того, як вони завдадуть реальної шкоди. Це робить їх важливим елементом загальної архітектури інформаційної безпеки організації [20].

2.2. Огляд та порівняльний аналіз DLP-рішень

На ринку представлено велику кількість DLP-продуктів, що відрізняються функціональними можливостями, архітектурними підходами, рівнем інтеграції з іншими системами безпеки, а також ціновою політикою. Через це вибір відповідного рішення потребує ретельного аналізу з урахуванням специфіки діяльності підприємства, типів оброблюваних даних, масштабів інфраструктури та бюджету.

Щоб краще зрозуміти, у чому полягають основні відмінності між такими рішеннями, розглянемо кілька конкретних прикладів.

Порівняємо чотири популярні DLP-системи: Symantec, McAfee, InfoWatch Traffic Monitor та Microsoft Purview (AIP/DLP).

Symantec Data Loss Prevention належить компанії Broadcom та є одним із найбільш функціонально насичених рішень на ринку засобів захисту від витоку даних. Цей продукт зарекомендував себе як стандарт корпоративного рівня, який широко застосовується у великих компаніях, державних установах та фінансових організаціях, де захист конфіденційної інформації має критичне значення.

Одна з ключових переваг Symantec DLP полягає в його глибокій інспекції вмісту (Deep Content Inspection), яка дозволяє не лише виявляти стандартні шаблони (наприклад, номери кредитних карток чи ідентифікаційні коди), а й аналізувати структуру документів, мовні конструкції та контекст використання інформації. Це дає змогу системі працювати з дуже низьким рівнем хибних спрацювань і високою точністю виявлення потенційно небезпечних передач даних.

Symantec забезпечує всебічне покриття каналів витоку − включаючи електронну пошту, веб-трафік, переносні носії, локальні файли на кінцевих пристроях, а також хмарні сервіси через інтеграцію з CloudSOC. Завдяки цьому організація отримує централізований контроль над усіма точками, де може статися витік інформації.

Важливим аспектом є також розширена система політик і класифікації даних, яка дозволяє створювати гнучкі правила залежно від типу інформації, користувача, його поведінки чи ризик-профілю. Адміністративна панель надає широкі можливості для кастомізації, аудиту й звітності.

Ще однією сильною стороною Symantec є можливість інтеграції з іншими продуктами Broadcom та системами управління безпекою, зокрема SIEM, IDM, та антивірусними рішеннями, що дозволяє побудувати комплексну архітектуру захисту.

Рішення є досить ресурсомістким, потребує часу на впровадження, професійної підтримки, а також значних інвестицій. З цієї причини воно більше підходить для великих організацій з розвиненими IT-командами та високими вимогами до контролю над інформацією.

Таким чином, Symantec DLP − це вибір для тих компаній, які потребують максимальної точності, гнучкості та контролю, й готові інвестувати у побудову системи захисту корпоративного рівня.

McAfee Total Protection for Data Loss Prevention входить до платформи Trellix, є популярним рішенням для комплексного захисту даних в організаціях середнього та великого рівня. Цей продукт поєднує перевірений часом підхід до запобігання витокам інформації з високим рівнем інтеграції в корпоративну інфраструктуру, особливо в екосистему McAfee/Trellix.

Однією з ключових переваг McAfee DLP є тісна інтеграція з платформою управління ePolicy Orchestrator (ePO), яка забезпечує централізоване управління всіма політиками безпеки, спрощує адміністрування та дозволяє ефективно координувати дії між різними компонентами системи захисту. Це особливо зручно для організацій, які вже використовують інші рішення McAfee, такі як антивірус, EDR або захист поштових серверів.

McAfee DLP охоплює ключові канали витоку інформації: електронну пошту, веб-з'єднання, зовнішні пристрої, буфер обміну, локальні файли, а також

друк. Також підтримується аналіз вмісту файлів за допомогою шаблонів, ключових слів, регулярних виразів і цифрових відбитків (fingerprinting), що дозволяє виявляти як явні, так і приховані витоки чутливих даних.

Важливою рисою є можливість захисту кінцевих точок (endpoint DLP), навіть коли пристрій працює в офлайн-режимі. McAfee також підтримує реактивні дії на інциденти, наприклад, блокування операцій, шифрування файлів, сповіщення користувача або адміністратора.

З технічного боку McAfee DLP вважається збалансованим рішенням, яке пропонує добрий компроміс між функціональністю та простотою налаштування. Адміністративний інтерфейс не такий інтуїтивний, як у деяких конкурентів, але добре знайомий фахівцям, які працювали з іншими продуктами McAfee.

Серед недоліків можна відзначити трохи обмежені можливості інтеграції з хмарними сервісами, у порівнянні з новітніми cloud-native DLP-рішеннями, та менш гнучкий підхід до поведінкової аналітики, яка реалізована на базовому рівні.

У підсумку, McAfee (Trellix) DLP є ефективним вибором для компаній, що прагнуть інтегрованого підходу до захисту даних, особливо якщо вони вже використовують інші продукти в рамках Trellix-екосистеми. Це рішення забезпечує надійний контроль над даними при помірних витратах на впровадження та підтримку, зокрема в корпоративних середовищах з великою кількістю кінцевих тЯчок.

InfoWatch Traffic Monitor - потужна корпоративна система захисту від витоків інформації, яка поєднує можливості класичної DLP з аналітикою поведінки користувачів (UEBA), моніторингом активності персоналу та розширеною мовною обробкою даних. Продукт орієнтований на виявлення несанкціонованого доступу, витоку або передачі конфіденційної інформації як через зовнішні канали (електронна пошта, месенджери, USB), так і у внутрішньому корпоративному середовищі.

Однією з ключових особливостей InfoWatch є глибока семантична обробка контенту, що дозволяє аналізувати не лише формальні ознаки витоку, а й зміст

повідомлень з урахуванням контексту, стилістики, емоційної тональності. Завдяки власному лінгвістичному модулю та підтримці багатьох мов (зокрема російської, української, англійської) рішення ефективно розпізнає порушення навіть у неструктурованих даних.

Система підтримує повний контроль інформаційних каналів: мережевий трафік, електронну пошту, друк, знімні носії, голосові дзвінки, відео, та дії користувача на робочому місці (наприклад, знімки екрана або натискання клавіш). Всі ці дані можуть аналізуватися в реальному часі або зберігатися для подальшого розслідування інцидентів. Крім того, InfoWatch має можливості інтеграції з SIEM-системами, каталогами Active Directory, CRM, ERP, системами документообігу, що дозволяє будувати комплексну архітектуру захисту.

У частині поведінкового аналізу InfoWatch дозволяє будувати профілі нормальної активності користувачів і автоматично виявляти відхилення - наприклад, раптову зміну обсягу копійованих даних або звернення до незвичних систем. Це підвищує здатність рішення виявляти не лише зовнішні атаки, але й внутрішні загрози (інсайдери, зловмисні дії персоналу).

Впровадження InfoWatch зазвичай вимагає системної інтеграції та глибокого налаштування політик, але після початкової конфігурації рішення демонструє високу точність та низький рівень хибних спрацювань. Варто врахувати, що продукт орієнтований переважно на великі та середні підприємства, особливо в тих країнах, де важливо зберігати дані на локальних серверах згідно з вимогами національного законодавства.

Microsoft Purview Data Loss Prevention - це сучасне рішення, що забезпечує захист конфіденційної інформації в межах хмарного середовища Microsoft 365, а також на рівні локальних пристроїв. Це рішення є наступником раніше відомої платформи Azure Information Protection (AIP) і нині інтегрується в ширший портфель Microsoft Purview − платформи для управління ризиками, даними та відповідністю.

Основна ідея цього рішення полягає у поєднанні автоматизованої класифікації даних, захисту кінцевих точок та централізованого управління політиками.

Purview дозволяє виявляти конфіденційну інформацію у таких середовищах, як Outlook, OneDrive, Teams, SharePoint та Exchange Online, без встановлення додаткового програмного забезпечення. Через механізм так званих “чутливих міток” (sensitivity labels) система може автоматично класифікувати документи, застосовувати до них шифрування, обмежувати доступ або блокувати певні дії, як-от друк або пересилання.

Завдяки інтеграції з Microsoft Defender та Insider Risk Management, платформа здатна не лише захищати дані, але й оцінювати ризики з боку користувачів - наприклад, за підозрілою поведінкою або ознаками витоку інформації. DLP на рівні кінцевих пристроїв працює у Windows-середовищі та дозволяє контролювати дії з файлами навіть в офлайн-режимі, включаючи копіювання на USB-носії, буфер обміну чи скриншоти.

Одним з основних плюсів Microsoft Purview є його глибока інтеграція в інфраструктуру Microsoft як у хмарі, так і в локальному середовищі. Це дозволяє впровадити захист без серйозних змін в існуючій IT-структурі, особливо якщо організація вже користується Microsoft 365. У той же час, цей же аспект обмежує гнучкість рішення - воно значно менш ефективне у середовищах, де домінують не-Microsoft продукти. Крім того, розгортання та налаштування можуть викликати складнощі у менш досвідчених адміністраторів, через велику кількість сервісів та інтерфейсів: Compliance Center, Purview Portal, Microsoft Defender тощо.

Ще однією проблемою це вартість, повноцінна функціональність доступна переважно у дорогих корпоративних ліцензіях, таких як Microsoft 365 E5. Це може обмежити доступ до найсучасніших можливостей захисту для малого або середнього бізнесу.

У цілому Microsoft Purview DLP технологічно просунуте рішення, створене передусім для організацій, глибоко інтегрованих у хмарну екосистему Microsoft. Воно забезпечує високий рівень автоматизації, відповідає міжнародним стандартам безпеки та є ефективним інструментом для централізованого управління ризиками, даними та дотриманням політик захисту інформації.

Підсумовуючи результати аналізу, можемо скласти порівняльну таблицю, де буде видно основні відмінності між DLP-рішеннями від різних постачальників, табл 2.1.

Таблиця 2.1

Порівняння DLP-рішень

Продукт / Критерій	**Symantec (Broadcom)**	**McAfee (Trellix)**	**InfoWatch Traffic Monitor**	**Microsoft Purview (AIP/DLP)**
Фокус рішення	Контроль даних і точна інспекція вмісту	Захист кінцевих точок, централізоване управління	Глибокий контент-аналіз, контроль поведінки, локальні вимоги	Хмарна інтеграція, автоматичне маркування, захист у Microsoft 365
Канали захисту	Email, Web, Endpoint, Cloud, Network	Email, Web, Endpoint, локальні дії, USB	Email, Web, Endpoint, принтери, USB, VoIP, месенджери, дії користувачів	Outlook, OneDrive, SharePoint, Teams, Windows Endpoint
Підхід до класифікації	Deep Content Inspection, шаблони, контекст	Шаблони, регулярні вирази, цифрові відбитки	Лінгвістичний аналіз текстів, семантика, словники, шаблони	Sensitivity Labels, автоматичне шифрування, класифікація за політиками
UEBA аналіз поведінки	Обмежено	Частково через XDR/SIEM	Потужна поведінкова аналітика, побудова профілів активності	Через Insider Risk Management та інтеграцію з Microsoft Defender

продовження таблиці 2.1

Інтеграція з іншими системами	SIEM, CASB, CloudSOC, Broadcom-сервіси	Повна інтеграція з ePO, сумісність з SIEM	SIEM, AD, ERP, CRM, документообіг, телефонія	Інтеграція з Defender, Sentinel, Microsoft 365, AIP, Microsoft Graph API
Захист хмари / SaaS	Через CloudSOC (Microsoft 365, Box, Google)	Обмежена інтеграція з хмарою	Обмежено - фокус на локальну інфраструктуру	Глибока інтеграція з Microsoft 365, хмара як основа платформи
Інтерфейс адміністратора	Потужний, але складний для новачків	Класичний інтерфейс через ePO	Складний, технічний, адаптований до великого бізнесу	Сучасний, проте фрагментований між порталами (Purview, Compliance Center тощо)
Гнучкість політик	Висока, широкі можливості кастомізації	Стандартизована політика	Дуже висока, сценарії адаптуються до галузі та внутрішньої структури	Висока в межах екосистеми Microsoft, менш ефективна за її межами
Рівень хибних спрацювань	Низький (за належного налаштування)	Середній	Низький, завдяки семантичному аналізу та контексту	Низький, при правильному налаштуванні класифікацій та міток
Простота впровадження	Складне, потребує досвіду і ресурсів	Порівняно просте (особливо для існуючих користувачів McAfee)	Просте для Microsoft-орієнтованих компаній	Просте для Microsoft-орієнтованих компаній, складне поза екосистемою

продовження таблиці 2.1

Тип організацій	Великі підприємства, банки, держустанови	Середній та великий бізнес, корпоративні IT-відділи	Компанії, які працюють у Microsoft 365, державні, освітні установи	Компанії, які працюють у Microsoft 365, особливо у хмарному або гібридному середовищі

2.3. Переваги та недоліки використання DLP в підприємстві

Підсумовуючи отриману інформацію можемо сказати, що використання DLP-технологій має як переваги, так і недоліки, які варто ретельно враховувати при впровадженні цих систем.

Однією з ключових переваг є можливість захисту конфіденційної інформації від несанкціонованого витоку. DLP-рішення дозволяють виявляти, контролювати та блокувати передачу чутливих даних, таких як фінансова інформація, персональні дані або комерційна таємниця, через різні канали, як електронну пошту, зовнішні носії, хмарні сервіси тощо. Це не лише підвищує загальний рівень інформаційної безпеки в організації, а й допомагає дотримуватись нормативних вимог як GDPR, HIPAA та інших.

DLP-системи можуть інтегруватися з іншими інструментами кібербезпеки, такими як SIEM, що дає змогу побудувати комплексну систему моніторингу та захисту.

Не звачаючи на це, DLP-рішення мають і свої недоліки. Одним з головних є складність впровадження та налаштування. Системи DLP вимагають чіткої класифікації даних і формування політик безпеки, що потребує значних часових і людських ресурсів. Неправильно налаштовані правила можуть спричинити як "хибні спрацювання", так і пропущені інциденти. Також варто враховувати, що деякі DLP-рішення можуть мати негативний вплив на швидкодію систем, особливо при моніторингу великого обсягу трафіку або файлів.

Не менш важливим є й фінансовий аспект. Повноцінна DLP-система це дорогий інструмент як з точки зору закупівлі, так і підтримки. Малі та середні підприємства часто не мають достатніх ресурсів для впровадження повного спектра функцій DLP.

Висновки до розділу 2

1. DLP (Data Loss Prevention) − це система запобігання втраті даних, яка захищає конфіденційну інформацію від несанкціонованого доступу, витоку або крадіжки. Вона здійснює протидію як випадковим, так і навмисним витокам, включаючи передачу даних у хмарні сховища. Замість жорстких блокувань використовуються політики, що дозволяють безпечні дії.

2. Основне призначення DLP-систем це захист від витоку конфіденційної інформації (випадкового або навмисного) та контроль таких потоків даних (Електронна пошта, HTTP-трафік, файли друку, тіньові копії файлів тощо).

Є три основні функції DLP-систем: ідентифікація, захист та реагування на загрози, пов'язані з конфіденційною інформацією. Може бути виконано за допомогою моніторингу, попередження користувача та блокування.

Також є інші функції окрім загальних: контроль передачі даних по протоколу FTP, контроль HTTP трафіку, контроль безпровідних мереж, інтеграція з Proxy-серверами, контроль обміну повідомленнями через соціальні мережі, розгортання у віртуальному середовищі, сканування робочих станцій, контроль буферу обміну, контроль баз даних та мережевих сховищ, інтеграція з LDAP, інтеграція з системами документообігу.

Ключові характеристики DLP − це глибокий аналіз вмісту, централізоване управління політиками, широке покриття даних на різних платформах.

Типи DLP-рішень: повноцінні − повне покриття мережі, сховищ і кінцевих точок; часткові − охоплюють два канали (наприклад, мережу та сховища) з повним робочим процесом; одноканальні − контроль лише одного каналу (мережа

або кінцеві точки); функції DLP в інших продуктах − обмежені можливості, інтегровані в інші продукти (наприклад, міжмережеві екрани).

DLP-системи можна поділити на три групи: на основі використання агента (agent based), без використання агента (agentless) та гібридні або змішані (hybrid).

3. Політики це основа DLP. Вони визначають різницю між публічними та конфіденційними даними. Створюються на основі внутрішніх вимог організації та зовнішніх стандартів. Залучають усі відділи компанії, особливо працівників, які безпосередньо працюють з даними.

Об’єктами контролю DLP є інтернет-трафік, документи, зовнішні носії, роздруковані матеріали, передані дані через Bluetooth, WiFi тощо.

Методи виявлення витоків проактивні та реактивні

Проактивні методи (аналіз вмісту): морфологічний аналіз − пошук ключових слів або фраз у тексті; статистичний аналіз − імовірнісна оцінка конфіденційності тексту на основі навчання алгоритмів; регулярні вирази (шаблони) − пошук за шаблонами (наприклад, номери кредитних карток, ID-документів).

Реактивні методи (ідентифікація за ознаками): цифрові відбитки − аналіз унікальних характеристик документа або його фрагментів, є можливість диференційованих дій залежно від ступеня збігу; цифрові мітки − спеціальні мітки, нанесені на документи, які визначають правила доступу.

4. Велика кількість DLP-продуктів, що відрізняються функціональними можливостями, архітектурними підходами, рівнем інтеграції з іншими системами безпеки, а також ціновою політикою.

Symantec Data Loss Prevention від Broadcom − корпоративне рішення для захисту даних з глибокою інспекцією вмісту та точним виявленням загроз. Забезпечує контроль над усіма каналами витоку та гнучку політику класифікації. Інтегрується з іншими продуктами Broadcom, SIEM та IDM. Потребує значних ресурсів і підходить для великих організацій з високими вимогами до безпеки.

McAfee Total Protection for DLP-рішення для середніх і великих компаній, інтегроване з ePolicy Orchestrator для централізованого управління. Підтримує основні канали витоку, аналіз вмісту, endpoint DLP та реакцію на інциденти. Має

збалансовану функціональність і підходить для користувачів екосистеми Trellix. Мінуси: обмежена хмарна інтеграція та базова поведінкова аналітика.

InfoWatch Traffic Monitor поєднує захист від витоків з аналізом поведінки користувачів і глибокою мовною обробкою. Система враховує контекст і зміст повідомлень, підтримує контроль усіх каналів передачі даних та дій на робочому місці. Наявна можливість виявляти відхилення від звичної поведінки дозволяє ефективно реагувати на внутрішні загрози. Рішення добре інтегрується в корпоративну інфраструктуру та підходить для середніх і великих компаній з вимогами до локального зберігання даних.

Microsoft Purview DLP-рішення для захисту конфіденційної інформації в екосистемі Microsoft 365. Воно поєднує автоматичну класифікацію, захист кінцевих точок і централізоване управління політиками. Завдяки глибокій інтеграції з іншими сервісами Microsoft, платформа ефективна в організаціях, що вже використовують цю інфраструктуру. Основні недоліки обмежена гнучкість поза середовищем Microsoft, складність налаштування та висока вартість повного функціоналу. Найбільш підходить для середніх і великих компаній, орієнтованих на хмарні сервіси Microsoft.

5. Переваги DLP-систем: ефективно захищають конфіденційні дані від витоку, забезпечуючи контроль над їх передачею через різні та допомагаючи дотримуватись вимог нормативів; вони можуть інтегруватися з іншими системами безпеки (наприклад, SIEM) для створення комплексного захисту.

Недоліки: DLP-рішення складні у впровадженні й налаштуванні, потребують точного визначення політик і значних ресурсів; можливі хибні спрацювання або пропуски, а також навантаження на систему; повноцінна DLP-система це значні фінансові витрати, що ускладнює її застосування в малому та середньому бізнесі.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

3.1. Опис та загальна характеристика підприємства

З метою наближення подальших досліджень до умов роботи реального підприємства, для зручності проведення досліджень, інтерпретації та демонстрації їх результатів, нами було навмання обрано відоме виробниче підприємство − Акціонерне товариство «Житомирський маслозавод» − компанія «Рудь» − далі Підприємство. Це один із провідних українських виробників харчових продуктів, зокрема морозива, вершкового масла, молочних виробів і заморожених продуктів.

Підприємство було засновано у 1937 році, а з 2003 року функціонує під торговельною маркою «Рудь», яка отримала широку популярність серед споживачів як в Україні так і за її межами. Компанія має сучасну виробничу інфраструктуру, потужні логістичні ланцюги, ефективну систему управління якістю, а також впроваджує інноваційні технології не тільки у виробничі процеси, а й в системи управління якістю та безпечністю продукції, менеджменту та логістичні процеси, які містять багато конфіденційної інформації.

Основні напрямки діяльності підприємства включають:

Виробництво морозива − основний сегмент діяльності. Асортимент продукції нараховує сотні позицій у різних формах, смаках та видах пакування.

Випуск вершкового масла та інших молочних продуктів, таких як згущене молоко, кисломолочні напої, сметана тощо.

Переробка та фасування заморожених овочів, ягід, грибів, картоплі фрі, а також виготовлення готового до приготування тіста.

Зберігання та дистрибуція продукції з використанням власних холодильних складів і автотранспорту з дотриманням температурного режиму.

Підприємство має розвинену організаційно-функціональну структуру, яка включає виробничі цехи, відділ контролю безпечності та якості продукції, IT-відділ, логістичний департамент, службу безпеки, кадровий, маркетинговий і фінансово-економічний відділи.

Система управління підприємством базується на принципах системності, стандартизації та безперервного вдосконалення, що дозволяє забезпечувати стабільну якість продукції, дотримання вимог законодавства, а також ефективне функціонування інформаційної інфраструктури.

Особливу увагу компанія приділяє інформаційній безпеці та захисту конфіденційної інформації, оскільки її діяльність пов'язана із збереженням персональних даних клієнтів, комерційною та технологічною інформацією. У цьому контексті підприємство впроваджує сучасні технічні та організаційні заходи з кібербезпеки, резервного копіювання, шифрування та захисту від внутрішніх і зовнішніх загроз.

Таким чином, Підприємство є комплексним об'єктом дослідження, що поєднує високотехнологічне виробництво харчових продуктів, цифрову інфраструктуру, багаторівневу систему управління та заходи інформаційної безпеки, що робить його придатним для аналізу у межах тематики цієї кваліфікаційної роботи, присвяченої захисту підприємства від витоку конфіденційної інформації.

До конфіденційної інформації досліджуваного підприємства належить широкий спектр відомостей, які мають обмежений доступ та потребують захисту від витоку за межі цифрових ресурсів підприємства відповідно до внутрішніх політик як самого підприємства, так і вимог чинного законодавства України та міжнародних стандартів інформаційної безпеки.

До основних категорій конфіденційної інформації, що обробляється на підприємстві, належать:

- *персональні дані працівників та клієнтів,* зокрема:

паспортні дані, ідентифікаційні коди, адреси проживання; дані про освіту, досвід роботи, стан здоров'я; банківські реквізити, контактна інформація;

- *інформація,* що збирається при взаємодії з веб-сайтами та цифровими сервісами компанії;
- *комерційна таємниця*, яка включає рецептури харчових продуктів та технологічні карти виробництва; інформацію про постачальників сировини, договірні умови; дані про логістичні маршрути, обсяги закупівель та продажів; внутрішню звітність, бізнес-плани, стратегії розвитку; результати маркетингових досліджень та аналізу конкурентів.
- *фінансова інформація* − бухгалтерська та податкова звітність; банківські виписки, дані про прибутки та витрати; внутрішні бюджети, прогнози та плани фінансування.
- *інформація про IT-інфраструктуру підприємства* − структура внутрішньої комп'ютерної мережі; IP-адреси серверів, логіни та паролі адміністраторів; налаштування систем безпеки, доступи до баз даних та CRM-систем; алгоритми шифрування, політики доступу, архіви журналів подій.
- *інформація про розробки та інновації* − результати науково-технічних розробок та досліджень; нові продукти, що перебувають у стадії тестування; патентна документація, заявки на реєстрацію торговельних марок.

Уся ця інформація підлягає обмеженому доступу, використовується лише уповноваженими особами та захищається від витоку за допомогою технічних і організаційних засобів безпеки, зокрема політик контролю доступу, резервного копіювання, антивірусного захисту, використання систем виявлення вторгнень.

Обробка та захист конфіденційної інформації на підприємстві здійснюється відповідно до чинного законодавства України, зокрема:

- ЗУ «Про інформацію» − визначає правові основи доступу до інформації, її класифікацію, включаючи комерційну таємницю та персональні дані;
- ЗУ «Про захист персональних даних» − регламентує порядок збору, зберігання, обробки та захисту персональних даних фізичних осіб;
- Господарський кодекс України − містить положення щодо збереження комерційної таємниці та відповідальності за її розголошення;

- ЗУ «Про електронні довірчі послуги» − встановлює вимоги до електронних підписів, шифрування та електронного документообігу;
- внутрішні положення, інструкції та політики підприємства, які конкретизують правила поводження з конфіденційною інформацією.

Практичні заходи захисту від витоку конфіденційної інформації

На підприємстві впроваджено комплекс заходів для забезпечення захисту інформації на організаційному, технічному та програмному рівнях:

- організаційні заходи: укладання з працівниками угод про нерозголошення (NDA); обмеження доступу до інформації за принципом «необхідності знання»; призначення відповідальних осіб за інформаційну безпеку; регулярне навчання персоналу з питань ІБ та поводження з даними.
- технічні засоби захисту: багаторівнева система авторизації доступу до внутрішніх ресурсів; використання фаєрволу, проксі-серверів та систем контролю трафіку; фізичний контроль за доступом до серверних приміщень (відеоспостереження, магнітні замки, обмеження за RFID-картками); резервне копіювання даних зберігається у захищеному середовищі.
- програмні рішення: впровадження DLP-систем для виявлення та блокування несанкціонованого виведення конфіденційної інформації; антивірусне ПЗ та системи виявлення шкідливого коду (SIEM/IDS/IPS); шифрування чутливої інформації на серверах і у транспортному середовищі (SSL/TLS, PGP); контроль за знімними носіями та зовнішніми підключеннями.
- інформаційна політика підприємства: політика безпечного використання мережевих та електронних сервісів;

регламент з поводження з електронною поштою та хмарними сховищами; аудит інформаційних систем з фіксацією інцидентів безпеки. Отже, за результатами вивчення роботи Підприємства встановлено, що воно приділяє значну увагу захисту інформаційних активів, оскільки втрата чи витік даних можуть призвести до зниження конкурентоспроможності, фінансових збитків або репутаційних ризиків.

Реалізація ефективної політики безпеки базується на поєднанні правового регулювання, технічних рішень та постійного підвищення обізнаності персоналу.

3.2. Аналіз загроз та вразливостей

Було досліджено роботу всіх виробничих цехів та офісних відділів Підприємства, встановлено, що Підприємство може мати як зовнішні загрози, так і внутрішні причини витоку КІ.

До зовнішніх загроз варто віднести кібератаки, тобто спроби зловмисників проникнути в ІТ-системи підприємства з метою викрадення або шифрування даних (наприклад, за допомогою вірусів, шкідливого ПЗ, фішингу). Зовнішні спроби обманом змусити працівників надати доступ до систем або розкрити чутливу інформацію, можуть відбуватися за допомогою розсилки фішингових листів. А використовуючи DDoS-атаки зовнішні зловмисники, в тому числі конкуренти, можуть порушити нормальне функціонування сервісів підприємства.

Але до витоку КІ призводять не тільки зовнішні атаки, але й внутрішні порушення політик Підприємства. Наприклад, недобросовісні працівники можуть навмисно копіювати, продавати або передавати КІ третім особам. Серед внутрішніх загроз витоку КІ варто відмітити зловживання правами доступу, тобто отримання доступу до даних, що не входять до кола посадових обов’язків співробітника.

Недостатня лояльність персоналу також може бути причиною витоку КІ. Така небезпека виникає у разі низької мотивації працівників або їх незадоволеності умовами праці.

Поряд із злонавмисною загрозою варто відмітити і ненавмисні причини витоку КІ, а саме людський фактор, тобто випадкове пересилання листа не тій особі, прикріплення неправильного файлу тощо, відправка файлів, що містять КІ на особисту пошту з метою доопрацювання у позаробочий час тощо.

До випадкових загроз витоку КІ слід віднести і недостатню обізнаність персоналу, що призводить до порушення політик інформаційної безпеки через необізнаність. Крім того, до переліку можливих загроз витоку КІ варто віднести і можливість технічних збоїв, а саме програмні помилки, відсутність шифрування резервних копій, використання застарілого ПЗ.

Вразливості інформаційної системи може підвищуватися через відсутність сучасних засобів виявлення аномалій трафіку (SIEM/IDS/IPS), використання застарілих ОС або програмного забезпечення. Недостатньо розмежовані рівні доступу, відсутність автоматизованого контролю за знімними носіями та мобільними пристроями або відсутність регулярних аудитів безпеки також варто віднести до високих ризиків витоку КІ.

Отже, для ефективного захисту Підприємства від витоку інформації необхідно враховувати не лише зовнішні атаки, а й внутрішні загрози та ризики, пов’язані з людським фактором. Застосування систем контролю доступу, шифрування, політик управління пристроями та DLP-рішень є критично важливим для запобігання витокам даних та збереження конкурентних переваг компанії.

3.3. Вибір і обґрунтування DLP-рішення

Враховуючи те, що Підприємство володіє великою кількістю технологічної та комерційної інформації, включаючи рецептури, виробничі процеси, дані клієнтів і постачальників, фінансову звітність тощо захист цих даних від витоку є критично важливим.

У зв’язку з цим актуальним є впровадження DLP-системи, яка дозволить запобігти витоку конфіденційної інформації, як через зовнішні канали, так і в результаті внутрішніх загроз.

У сучасних умовах цифровізації виробничих процесів захист конфіденційних даних також стає критично важливим, а саме DLP-системи призначені для запобігання витоку інформації, контролю її обігу та забезпечення відповідності вимогам регуляторів.

У даному аналізі нами розглядаються чотири найбільш популярні DLP-рішення: "Symantec DLP", "Microsoft Purview (AIP/DLP)", "McAfee Total Protection DLP" та "InfoWatch Traffic Monitor".

Критерії порівняння включають функціональність, вартість, простоту впровадження, інтеграцію з інфраструктурою та рівень підтримки.

Для підприємства обрано такі ключові критерії вибору, табл. 3.1.

Таблиця 3.1

Ключові критерії вибору DLP-систем Підприємства

Критерій	**Опис**
Функціональність	Широта можливостей виявлення, блокування та контролю витоків
Ціна / Ліцензування	Вартість продукту, гнучкість у масштабуванні
Простота впровадження	Час, ресурси та складність налаштування
Інтеграція	Сумісність з ОС, серверами, поштовими системами, ERP
Підтримка та оновлення	Наявність технічної підтримки, регулярність оновлень

Було проведено порівняльний аналіз популярних DLP-продуктів, табл. 3.2.

Система «Symantec DLP» за критерієм «функціональність» пропонує потужні інструменти контролю даних, включаючи розширене шифрування та гнучкі механізми маркування інформації. Це робить її особливо корисною для організацій з високими вимогами до захисту даних.

Висока вартість обумовлена розширеними можливостями та індивідуальним підходом до налаштування. Простота впровадження, або в даному випадку складність інтеграції, пов'язана з потребою глибокого налаштування та адаптації під конкретні вимоги існуючого обладнання.

Таблиця 3.2

Порівняльна характеристика популярних DLP-продуктів

Назва DLP-системи	**Функціональність**	**Ціна/ Ліцензування**	**Простота впровадження**	**Інтеграція**	**Підтримка**
Symantec DLP	Потужна політика контролю, розширене шифрування	Висока	Складна	Широка (AD, Exchange, SaaS)	Високий рівень підтримки
Microsoft Purview (AIP/DLP)	Відмінна інтеграція з Microsoft 365	Включено у Microsoft E5	Проста для M365	Ідеальна для Microsoft-інфраструктури	Постійна підтримка
McAfee Total Protection DLP	Сильний endpoint-контроль, аудити	Середня	Помірна складність	Windows, macOS, мережі, пошта	Надійна підтримка
InfoWatch Traffic Monitor	Потужний аналіз трафіку, контроль мовних моделей	Середня/висока	Середня складність	Серверні мережі, пошта, документообіг	Локалізована підтримка

Система «Symantec DLP» підтримує широкий спектр систем, включаючи Active Directory, Exchange та SeaS, що дозволяє легко інтегрувати її в існуючу інфраструктуру. А високий рівень підтримки забезпечує оперативне вирішення проблем та консультації.

Система Microsoft Purview (AIP/DLP) - це ідеальний вибір для підприємств, які використовують Microsoft 365, оскільки вона пропонує повну інтеграцію та комплексні інструменти захисту даних.

Система має невисоку вартість впровадження, оскільки її включено у пакет Microsoft E5, що робить його економічно вигідним для клієнтів Microsoft.

Простий у використанні для середовищ Microsoft 365, але може вимагати додаткових зусиль для інших платформ.

Система Microsoft Purview (AIP/DLP) є оптимальною для Microsoft-інфраструктури з обмеженою підтримкою сторонніх систем.

Постійна підтримка від Microsoft забезпечує надійність та стабільність роботи.

Система McAfee Total Protection DLP виділяється сильним контролем endpoint-пристроїв та можливостями аудиту, що важливо для виробничих підприємств з розподіленою інфраструктурою.

Середній рівень цін робить її доступною для середніх та великих компаній.

Середня складність впровадження, пов'язана з необхідністю налаштування політик безпеки.

Система McAfee Total Protection DLP підтримує Windows, macOS, мережі та поштові системи, що забезпечує її гнучкість у використанні.

Надійна підтримка від McAfee дозволяє швидко вирішувати технічні питання.

Система InfoWatch Traffic Monitor спеціалізується на аналізі трафіку та контролі мережевих потоків, що є ключовим для виявлення аномалій та запобігання витоку даних. Система має від середнього до високого рівень цін, залежно від масштабів впровадження. Середня складність її інтеграції пов'язана з налаштуванням моніторингу мережевого трафіку.

Система InfoWatch Traffic Monitor підтримує серверні мережі, поштові системи та документообіг, що робить її придатною для комплексного захисту, а локалізована підтримка може бути корисною для україномовних клієнтів.

Отже, для будь якого підприємства, яке потребує надійного захисту конфіденційних даних та інтеграції з існуючою інфраструктурою, рекомендуються наступні варіанти:

1. Microsoft Purview: Якщо підприємство використовує Microsoft 365, це рішення є оптимальним через низьку вартість (включено в E5), простоту інтеграції та високу якість підтримки.

2. Symantec DLP: Якщо потрібен високий рівень контролю та шифрування, незважаючи на високу вартість та складність впровадження.

3. McAfee Total Protection DLP: для підприємств з розподіленою інфраструктурою, де важливий контроль endpoint-пристроїв.

А для Підприємства, з його орієнтацією на Microsoft-інфраструктуру, найбільш підходить DLP-система "Microsoft Purview".

У випадку потреб у розширеному контролі та шифруванні варто розглянути "Symantec DLP".

Для балансу між функціональністю та вартістю можна обрати "McAfee Total Protection DLP".

Microsoft Purview DLP − найбільш доцільне рішення для впровадження на Підприємстві з огляду на:

- інтеграцію з Microsoft 365, яка вже використовується в більшості офісів компанії;
- можливість контролю конфіденційних даних у листах, документах, хмарах, Teams;
- знижену вартість впровадження, оскільки більшість функцій входять у пакет Microsoft 365 E5 або можуть бути ліцензовані окремо;
- просте адміністрування, зокрема для IT-відділу підприємства, без потреби розгортання складної інфраструктури;
- автоматизовані правила DLP: наприклад, блокування відправлення листів із вмістом, що містить фінансову звітність або персональні дані.

Отже, впровадження DLP-системи Microsoft Purview дозволить ефективно забезпечити безпеку критичної інформації Підприємства. Рішення відповідає сучасним вимогам, є економічно вигідним та адаптованим до наявної IT-інфраструктури компанії.

Як альтернатива, при наявності складної мережевої архітектури або вимог до глибокого аналізу трафіку, доцільно розглядати InfoWatch або McAfee DLP.

3.4. Модель впровадження DLP на підприємстві

Для поетапного впровадження DLP-системи Microsoft Purview на Підприємстві нами розроблено модель впровадження, яку можна представити у графічному вигляді, що складається з двох основних етапів (рис. 3.1).

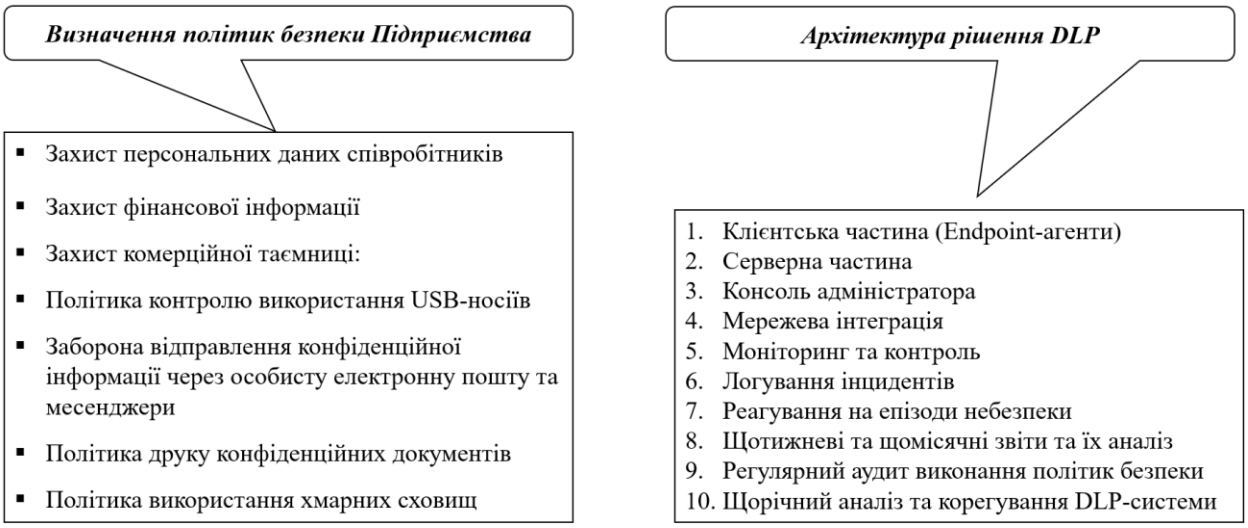

Рисунок 3.1 – Модель поетапного впровадження DLP-системи «Microsoft Purview» на Підприємстві

На першому етапі формуються політики безпеки відповідно до потреб підприємства, з урахуванням законодавчих вимог,а також специфіки діяльності.

До основних політик безпеки DLP-системи Підприємства нами було включено:

- захист персональних даних співробітників (ПІБ, ІПН, паспортні дані, зарплатна інформація);
- захист фінансової інформації (бюджети, звіти, рахунки, банківські реквізити);

- захист комерційної таємниці (рецептури морозива та молочних продуктів;

дані про технологічні процеси; контракти з постачальниками і дистриб'юторами);

- політика контролю використання USB-носіїв (заборона або шифрування);
- заборона відправлення конфіденційної інформації через особисту електронну пошту та месенджери;
- політика друку конфіденційних документів (контроль друку / обмеження);
- політика використання хмарних сховищ (Dropbox, Google Drive, iCloud − дозвіл / заборона).

Враховуючи те, що в результаті порівняльного аналізу популярних DLP-систем нами було обрано систему Microsoft Purview DLP на другому етапі впровадження ми пропонуємо наступну архітектуру, яка передбачає багаторівневий поступовий підхід.

Першим кроком обрано налаштування клієнтської частини (Endpoint-агенти): яка встановлюються на комп'ютери співробітників (бухгалтерія, ІТ-відділ, комерційний відділ, лабораторія тощо).

Особлива увага приділяється інструктажу робітників Підприємства щодо дотримання всіх політик безпеки підприємства, у тому числі контролю копіювання файлів, друку, USB, e-mail, месенджерів. З метою запобігання ненавмисних дій працівників, які можуть призвести до витоку КІ DLP-системою передбачена можливість блокування або повідомлення у разі порушення політик.

На другому кроці впровадження налаштовується серверна частина, а саме центральний DLP-сервер (фізичний або хмарний) для обробки, зберігання інцидентів та логів.

Третім кроком впровадження DLP-системи обрано консоль адміністратора, завданням якого є централізоване керування всіма політиками безпеки Підприємства та інцидентами. На цьому кроці також передбачена інтеграція DLP-системи з Active Directory, Microsoft Exchange, SharePoint, Teams (у разі використання Microsoft 365).

На четвертому кроці впровадження відбувається мережева інтеграція, яка передбачає налаштування моніторингу трафіку через шлюз/проксі-сервер.

П’ятим кроком є організація контролю даних, що передаються через Інтернет та налаштування моніторингу й реагування на тривожні сповіщення системи у разі порушень політик безпеки Підприємства. Моніторинг та постійний контроль усіх каналів передачі інформації забезпечують виявлення підозрілої поведінки працівників (наприклад, масове копіювання файлів, несанкціоноване використання USB).

Шостим кроком впровадження є логування інцидентів (хто, коли, що і яким чином намагався скопіювати, переслати чи зберегти КІ).

На сьомому кроці впровадження DLP-системи встановлено сценарії реагування на епізоди витоку КІ, а саме мають бути налаштовані автоматичні дії, такі як блокування операції, попередження користувача, сповіщення адміністратору та ручні дії − аналіз ситуації ІТ-відділом, проведення службового розслідування. У випадку встановлення факту витоку КІ DLP-система автоматично передає критичні інциденти до служби безпеки підприємства та керівництва.

Восьмим кроком впровадження DLP-системи є організація щотижневих та щомісячних звітів про події DLP-системи, завданням яких є систематизувати інформацію про витоки КІ, що дозволить формувати тренди та виявляти «вузькі місця» у захисті інформації, що сприяє запобіганню витоку КІ.

Для ефективної роботи DLP-системи передбачено дев’ятий крок впровадження, а саме у календарний план роботи Підприємства включається регулярний аудит виконання політик Підприємства та дисципліни працівників, частота якого корегується щорічно.

Заключний десятий крок впровадження передбачає планування щорічного аналізу та корегування DLP-системи Підприємства, що дозволить виявляти її сильні та слабкі місця та вчасно їх корегувати враховуючи зміни як нормативно-технічної бази та і можливості інформаційних технологій.

Розроблена модель дозволяє системно впровадити DLP-рішення на Підприємстві, з урахуванням технологічної інфраструктури, чутливої інформації та вимог до захисту даних. Вона забезпечить контроль за всіма потенційними каналами витоку інформації та дозволить запобігти втратам, пов'язаним із внутрішніми або зовнішніми загрозами.

Очікуваним ефектом від впровадження DLP-системи на Підприємстві є:

1. Підвищення рівня інформаційної безпеки Підприємства, а саме: забезпечення контролю за усіма каналами передавання та обробки чутливої інформації (внутрішні мережі, електронна пошта, зовнішні носії, хмарні сервіси); формування прозорої та контрольованої політики поводження з даними для всіх співробітників; унеможливлення несанкціонованого доступу або виведення критичної інформації (наприклад, рецептур, фінансових звітів, персональних даних працівників).

2. Зниження ризику витоку конфіденційної інформації.

Завдяки впровадженим механізмам моніторингу, блокування та оповіщення, ризики витоку інформації зменшуються в рази. Попередження як зовнішніх загроз (в результаті фішингових атак, хакерських зламів), так і внутрішніх порушень (ненавмисних або зловмисних дій працівників). Зменшення ймовірності фінансових та репутаційних збитків, пов'язаних із втратами критичних даних або порушенням договірних умов із партнерами.

3. Відповідність чинним нормативним вимогам.

Дотримання міжнародних стандартів безпеки інформації: ISO/IEC 27001 – Система менеджменту інформаційної безпеки; GDPR – Загальний регламент захисту даних ЄС (актуально для експорту продукції в Європу); Закон України «Про захист персональних даних». Спростить проходження аудитів з боку контролюючих органів та сертифікаційних структур. Підвищить рівень

довіри з боку клієнтів, партнерів і постачальників, що особливо важливо для компанії, яка активно працює на зовнішніх ринках.

4. Організаційна зрілість і підвищення культури безпеки.

Після впровадження DLP-системи компанія отримає централізовану систему контролю та інструменти управління інцидентами. Впровадження сприятиме формуванню усвідомленої поведінки співробітників у сфері обігу з інформацією. Знижується залежність від людського фактору - система автоматично реагує на загрози, незалежно від дій працівника.

Висновки до розділу 3

Встановлено, що для підвищення ефективності попередження витоку КІ на підприємстві доцільно використати систему попередження витоку КІ Microsoft Purview DLP, а саме з огляду на:

- інтеграцію всього ПЗ з Microsoft 365, який вже використовуэться;
- можливість контролю конфіденційних даних у листах, документах, хмарах, Teams;
- низьку вартість впровадження;
- просте адміністрування.

При подальшому удосконаленні мережевої архітектури або вимог до аналізу трафіку, можна розглядати продукти InfoWatch або McAfee DLP.

ВИСНОВКИ

1. Вивчено поняття КІ та основні загрози її витоку. Встановлено, що КІ - це інформація, доступ до якої обмежено, і яка має цінність для держави, юридичних чи фізичних осіб. Її розголошення може завдати шкоди публічним або приватним інтересам. Витік інформації може здійснюватися через помилки або збої в роботі елементів АС, фізичні пошкодження, недосконале або застаріле програмне забезпечення, людський фактор, технічні канали тощо. Джерелами загроз витоку КІ можуть бути: персонал, який працює з АС, технічні засоби й ПЗ, технології обробки інформації, природні чи штучні зовнішні фактори.

2. Досліджено методи захисту інформації, зокрема DLP-технологію. Встановлено, що Data Loss Prevention – це переважно програмне рішення, яке поєднує активні та пасивні засоби захисту інформації. Вона призначена для виявлення, моніторингу та запобігання несанкціонованому розповсюдженню конфіденційних даних всередині організації і за її межами. Особливо важлива для захисту чутливої інформації − персональних даних, комерційної таємниці, фінансових документів та інтелектуальної власності. Впровадження DLP-систем допомагає зменшити ризики витоків, що можуть призвести до фінансових, репутаційних і правових втрат.

3. Визначено переваги та недоліки впровадження DLP на підприємствах. Встановлено, що основною перевагою використання DLP-систем є ефективний захист КІ від витоку завдяки контролю над її передачею через різні канали руху інформації (email, носії, хмара) та можливість врахувати вимоги нормативних документів (GDPR, HIPAA тощо). DLP-системи можуть інтегруватися з іншими системами безпеки (наприклад, SIEM) для створення комплексного захисту.

До недоліків варто віднести складність у впровадженні й налаштуванні, які потребують точного визначення політик і значних ресурсів; можливі хибні спрацювання або пропуски, а також навантаження на систему. Також впровадження

повноцінної DLP-системи потребує значних фінансових витрат, що ускладнює її застосування в малому та середньому бізнесі.

4. Проведено порівняльний аналіз популярних DLP-рішень для підвищення ефективності попередження витоку конфіденційної інформації на Підприємстві. Встановлено, що система попередження витоку КІ Microsoft Purview DLP − є найбільш доцільним рішенням для впровадження на Підприємстві з огляду на: інтеграцію з Microsoft 365, яка вже використовується в більшості офісів компанії; можливість контролю конфіденційних даних у листах, документах, хмарах, Teams; знижену вартість впровадження, оскільки більшість функцій входять у пакет Microsoft 365 E5 або можуть бути ліцензовані окремо; просте адміністрування, зокрема для ІТ-відділу підприємства, без потреби розгортання складної інфраструктури; автоматизовані правила DLP: наприклад, блокування відправлення листів із вмістом, що містить фінансову звітність або персональні дані.

При подальшому удосконаленні мережевої архітектури або вимог до аналізу трафіку, можна розглядати InfoWatch або McAfee DLP.

5. Розроблено систему захисту конфіденційної інформації для Підприємства із використанням DLP-системи Microsoft Purview та запропоновано модель її поетапного впровадження, що дозволить ефективно упередити витоки КІ на Підприємстві. Рішення відповідає сучасним вимогам, є економічно вигідним та адаптованим до наявної ІТ-інфраструктури компанії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник / за ред. В. Г. Кривуци. Київ, 2004. 508 с.

2. Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації // Південноукраїнський правничий часопис, - 2021. - №1, - С. 94-98.

3. Антонюк А., Жора В. Загрози інформації і канали витоку // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. – Вип. 2. – С. 42-46.

4. Аль-Амморі А. Н., Дехтяр М.М., Іщенко Р.М., Клочан А.Є. Методи та засоби захисту інформації // Системи управління, навігації та зв’язку : зб. наук. пр. – 2024. – Вип. 1.75. –С. 38-44.

5. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

6. Про інформацію : Закон України від 15.11.2024 №4017-IX. Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650.

7. Про захист персональних даних : Закон України від 18.01.2025 р. №3980-IX. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481.

8. Про доступ до публічної інформації : Закон України від 08.10.2023 р. №2614-IX. Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314.

9. Про державну таємницю : Закон України від 30.10.2024 р. №4019-IX. Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93.

10. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР, № 31, ст.286.

11. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII, № 45, ст.400.

12. Про основні засади забезпечення кібербезпеки України : Закон України від 20.04.2025 р. №4336-IX. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.

13. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах

[Електронний ресурс]: Постанова КМУ від 29 березня 2006 р. № 373. – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

14. Кодекс України про адміністративні правопорушення : Відомості Верховної Ради УРСР від 07.12.1984 р. № 8073-X, № 51, ст. 1122.

15. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001. № 25-26. ст. 131.

16. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. [Чинний від 2023-10-01]. Вид. офіц. Київ, 2023. 37 с.

17. Про Положення про технічний захист інформації в Україні [Електронний ресурс]: Указ Президента України від 27.09.1999 р. № 1229/99. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text.

18. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. - [Чинний від 2021]. К.: Держспецзв'язку України, 2021. – 29 с.

19. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. Адміністрація Держспецзв'язку [Електронний ресурс]; Наказ, Рекомендації від 29.05.2023 № 463. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text.

20. Полотай О. І., Пузир А. О. Аналіз засобів запобігання витоку конфіденційної інформації на підприємствах, на прикладі системи DLP // Вісник Львівського державного університету безпеки життєдіяльності. – 2024. – № 30. – С. 134-144.

21. Cheng L., Liu F., Yao D. Enterprise data breach: causes, challenges, prevention, and future directions [Електронний ресурс] // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2017. Т. 7, № 5. Ст. e1211. – Режим доступу: https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1211.

22. Data Loss Prevention R76 Administration Guide. Introduction to Data Loss Prevention [Електронний ресурс]. Check Point Software Technologies Ltd. 2014. – Режим доступу: https://sc1.checkpoint.com/documents/R76/CP_R76_DLP_WebAdmin/62453.htm.

23. Torsteinbø T. Data loss prevention systems and their weaknesses // University of Agder. – 2012. – 87 с.

24. Gupta I., Mittal S., Tiwari A., Agarwal P., Singh A. K. TIDF-DLPM [Електронний ресурс]: Term and Inverse Document Frequency Based Data Leakage Prevention Model. 2022. – Режим доступу:https://arxiv.org/pdf/2203.05367.

25. Gupta K., Kush A. A Forecasting-Based DLP Approach for Data Security [Електронний ресурс] // Data Analytics and Management / за ред. A. Khanna, D. Gupta, Z. Pólkowski, S. Bhattacharyya, O. Castillo. Singapore. 2021. – Режим доступу: https://doi.org/10.1007/978-981-15-8335-3_1.

26. Hassan M., та ін. Implementation of security systems for detection and prevention of data loss/leakage at organization via traffic inspection [Електронний ресурс]. 2020. – Режим доступу: https://arxiv.org/pdf/2012.14111.

27. Daubner L., Považanec A. Data Loss Prevention Solution for Linux Endpoint Devices [Електронний ресурс]. 2023. – Режим доступу: https://dl.acm.org/doi/abs/10.1145/3600160.3605036.

28. Understanding and Selecting a Data Loss Prevention Solution [Електронний ресурс]. – Ver. 2.0. – Securosis, L.L.C., 2010. – Режим доступу: http://viewer.media.bitpipe.com/985719113_684/1294934983_394/whitepaper-understanding-and-selecting-a-data-loss-prevention-solution-en.pdf.

29. Gupta K., Kush A. A Learning Oriented DLP System Based on Classification Model [Електронний ресурс]. 2023. – Режим доступу: https://arxiv.org/abs/2312.13711.

30. Tanaka P., Sapra S., Laptev N. Scalable Data Classification for Security and Privacy [Електронний ресурс]. 2020. – Режим доступу: https://arxiv.org/abs/2006.14109v5.

31. Patil R., Pise, G., Bhosale Y. Root causes, ongoing difficulties, proactive prevention techniques, and emerging trends of enterprise data breaches [Електронний ресурс]. 2023. – Режим доступу: https://arxiv.org/abs/2311.16303.