МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ЗАСТОСУВАННЯ DLP-СИСТЕМ ЯК ІНСТРУМЕНТУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

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

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

_____ Денис ОДНООЧКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Денис ОДНООЧКО
Ім'я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., професор Ім'я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Одноочку Денису Володимировичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Застосування DLP-систем як інструменту забезпечення інформаційної безпеки”,
керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “__“ березня 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, розгляд існуючих загроз витоків інформації на підприємствах, системи запобігання витоку інформації, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Пояснення важливості забезпечення інформаційної безпеки на підприємствах, аналізуючи загрози витоків даних.
4.2. Проаналізувати DLP-системи та визначити принципи їх функціонування.
4.3. Розробити практичні рекомендації щодо впровадження системи запобігання витоку даних та надати пропозиції щодо підвищення стійкості існуючих DLP рішень.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання“11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Розгляд важливості забезпечення інформаційної безпеки на підприємствах, аналізуючи загрози витоків даних.	08.04.2024	
4.	Дослідження різновидів DLP-систем та визначення принципів їх роботи.	22.04.2024	
5.	Оцінювання сучасних DLP-систем шляхом проведення порівняльного аналізу та визначення загальних застережень при їх впроваджені.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Денис ОДНООЧКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Одноочко Д.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Застосування dlp-систем як інструменту забезпечення інформаційної безпеки "

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ОДНООЧКО Денис у кваліфікаційній роботі пояснив важливість забезпечення інформаційної безпеки на підприємствах, аналізуючи загрози витоків даних.

ОДНООЧКО Денис показав розуміння проблеми дослідження та описав концепцію вибору того чи іншого рішення запобігання витоку даних, шляхом визначення принципів їх функціонування.

ОДНООЧКО Денис довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ОДНООЧКА Дениса на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Одноочко Д.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ОДНООЧКА Дениса
на тему "Застосування DLP-систем як інструменту забезпечення інформаційної безпеки"

Актуальність. У світі, де держави, компанії та навіть окремі користувачі є об'єктами кібератак, важливість забезпечення інформаційної безпеки є великою, як ніколи. До того ж, ІТ-сфера постійно розвивається, і з цим зростають інформаційні ризики і загрози. В таких умовах варто приділити першочергове значення захисту конфіденційних даних.

З огляду на зазначене дослідження проблеми застосування DLP-систем як інструменту забезпечення інформаційної безпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено застосування DLP-систем як інструменту забезпечення інформаційної безпеки.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо впровадження системи запобігання витоку даних, а також надано пропозиції щодо підвищення їх стійкості.

Недоліки.

Доцільно було б приділити більше уваги порівняльному аналізу сучасних DLP-систем для вибору однозначного рішення, яке забезпечить комплексний захист конфіденційної інформації та безпеку даних у сучасних умовах цифрової трансформації.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а здобувач ОДНООЧКО Денис заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню використання DLP-систем як інструменту забезпечення інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 13 рисунків, висновків і списку використаних джерел із 16 найменувань. Загальний обсяг роботи становить 62 аркушів, з яких 3 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження DLP-систем для забезпечення інформаційної безпеки на підприємствах.

Об'єктом дослідження є системи запобігання витоку інформації різного виду й принципи їх функціонування.

Предмет дослідження **–** особливості DLP рішення для подальшого впровадження на підприємствах.

Методи дослідження**.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, експертної оцінки, системного підходу щодо вибору DLP рішення.

Як результат у роботі доведено важливість забезпечення інформаційної безпеки на підприємствах, проаналізовано DLP-системи та визначено принципи їх функціонування. Також розроблено практичні рекомендації щодо впровадження системи запобігання витоку даних та надано пропозиції щодо підвищення стійкості існуючих DLP рішень.

Галузь застосування**.** Розроблені рекомендації в результаті дослідження можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті впровадження DLP рішень.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, DLP-СИСТЕМИ.

ABSTRACT

The qualification work is devoted to the study of the use of DLP systems as a tool for ensuring information security. The work consists of an introduction, three chapters containing 13 figures, conclusions and a list of references of 16 titles. The total volume of the work is 62 pages, of which 3 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to study DLP systems to ensure information security at enterprises.

The object of the study is the systems for preventing information leakage of various types and the principles of their functioning.

The subject of the study is the features of DLP solutions for further implementation at the enterprise.

Research methods. To solve the above scientific task, the paper uses the methods of analysis, comparison, classification, expert evaluation, and a systematic approach to choosing a DLP solution.

As a result, the paper proves the importance of ensuring information security at enterprises, analyzes DLP systems and defines the principles of their functioning. Also, practical recommendations for implementing a data leakage prevention system are developed and proposals are made to improve the sustainability of existing DLP solutions.

Field of research. The developed recommendations as a result of the study can be used in the planning and implementation of an enterprise information security management system in the context of implementing DLP solutions.

Keywords: ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT, DLP SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

DCAP - Data-Centric Audit and Protection
DLP - Data Loss Prevention

GDPR - General Data Protection Regulation

HIPAA - Health Insurance Portability and Accountability Act

IPC - Inter-Process Communication

PCI - Payment Card Industry

PCI-DSS - Payment Card Industry Data Security Standard

PII - Personally Identifiable Information

SaaS - Software as a Service

SIEM - Security Information and Event Management

VDI - Virtual Desktop Infrastructure

ІБ - Інформаційна безпека

ІКС - Інформаційно-комунікаційні технології

ОС - Операційна система

ПЗ - Програмне забезпечення

ШІ – Штучний інтелект

ВСТУП

Актуальність теми. На сьогодні захист інформації від витоку є одною із найбільш актуальних тем. Прогресивний розвиток технологій і зростаюча кількість цифрової інформації робить її вразливою перед багатьма загрозами. Захист даних стає критичним як для окремих осіб, так і для підприємств у всіх сферах діяльності.

Захист даних як концепція кібернетичної безпеки не є новою, але вимоги, що висуваються до старих систем захисту даних, кардинально змінилися за останнє десятиліття. Колись фахівці з безпеки були впевнені, що цінні дані, які вони захищають, надійно заховані в добре укріплених центрах обробки даних. Але цифрова трансформація призводить до того, що великі та малі компанії переміщують свої дані в хмару та в розподілені місця. Ваші дані тепер доступні скрізь, де б не перебували користувачі. Ваш бізнес може ділитися цифровими зв'язками з величезною кількістю третіх сторін - постачальників, партнерів і підрядників. Такі сценарії приносять як безпрецедентні можливості для бізнесу (хороші новини), так і виклики для безпеки, особливо щодо захисту даних (не дуже хороші новини). Успішні зломи можуть мати руйнівні наслідки для бізнесу. Ризики з боку інсайдерів (зловмисних чи недбалих) так само небезпечні для вашого бізнесу, як і гучні атаки з боку зовнішніх гравців.

Усі вони загрожують витоком конфіденційної інформації. Захист даних зараз є наріжним каменем правил комплаєнсу, а галузеві правила та правила конфіденційності даних детально описують обов'язки вашого бізнесу та передбачають значні штрафи за їх невиконання. Компанії повинні прийняти новий підхід і застосовувати політику захисту даних скрізь, де є їхні дані - послідовно. В ідеалі, захист даних сприяє досягненню бізнес-цілей і водночас захищає бізнес. але управління політиками захисту даних та інструментами, необхідними для їх дотримання, може бути складним і дорогим. Підприємствам потрібні рішення для захисту даних, які спрощують впровадження політик і водночас забезпечують їхню ефективність. Нове покоління хмарних рішень для

запобігання втраті даних (DLP) пропонує можливий шлях вперед. Підприємства повинні прийняти хмарне рішення, яке є менш складним, масштабованим і більш економічно ефективним, а в ідеалі - захищає дані з більшою надійністю і точністю, а також мінімізує ризик несанкціонованого доступу до них з боку зовнішніх суб'єктів.

Метою роботи полягає у дослідженні DLP-систем для забезпечення інформаційної безпеки на підприємствах.

Об'єкт дослідження – системи запобігання витоку інформації різного виду й принципи їх функціонування.

Предмет дослідження – особливості DLP рішення для подальшого впровадження на підприємствах.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити загальні принципи забезпечення інформаційної безпеки, шляхом аналізування статистики витоку даних та існуючих каналів витоку.

2. Проаналізувати DLP-системи та дослідити принципи функціонування їх.

3. Порівняти сучасні рішення DLP, визначити застереження при впровадженні системи запобігання витоку даних та надати пропозиції щодо підвищення ефективності роботи цієї системи.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, експертної оцінки та системного підходу щодо вибору DLP-рішень.

Практичне значення одержаних результатів. Практичне значення одержаних в майбутньому результатів полягає у можливості застосування розроблених рекомендацій для ефективного впровадження DLP-систем на підприємствах. Це дозволить забезпечити надійний захист конфіденційної інформації від несанкціонованого доступу та витоку.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Розділ 1 ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

1.1 Важливість захисту інформації як цінного активу на підприємствах

Незалежно від форми власності та типу діяльності підприємства, інформація є ключовим аспектом для прийняття важливих управлінських рішень, таких як визначення ринкової стратегії, планування майбутнього розвитку, інвестування в проєкти та укладання угод.

Інформація може бути одним із найцінніших чинників, які приносять прибуток. Цю ситуацію можна проілюструвати на прикладі брокерських послуг з управління цінними паперами на міжнародних біржах. Будь-яка інформація, навіть неправдиві чутки, може миттєво змінити ситуацію на ринку. Наприклад, витік інформації про укладення угоди, судовий розгляд чи інсайдерські дані про новинки продукції може спричинити миттєве падіння або зростання акцій. Нові технології, інноваційні ідеї, виробничі ноу-хау та вихідний код програмного продукту – все це є інформацією, використання якої, як ресурсу суттєво впливає на кінцеві результати діяльності. Таким чином, інформація перестає бути просто даними і стає цінним активом компанії.

Оскільки вся інформація обробляється за допомогою інформаційних технологій, вона нерозривно пов'язана з обчислювальною технікою та працівниками, які її використовують. Таким чином, під інформаційними активами компанії розумітимемо всі цінні інформаційні ресурси власника, здатні приносити йому економічну вигоду, в яких накопичені знання, вміння та навички персоналу, та реалізовані з використанням сучасних інформаційних технологій. Іншими словами, інформаційні активи слід розглядати як нерозривну сукупність самої інформації, засобів її обробки та персоналу, які мають до неї доступ та безпосередньо її використовують. І, відповідно, кінцева вартість інформаційних активів також буде формуватися загальною вартістю всіх складових, описаних вище.

Оскільки наявні інформаційні активи, необхідно мати механізми для оцінки та обліку такого роду активів. Функцію обліку часто покладають на службу інформаційної безпеки, де процес обліку та оцінки є складовою частиною управління ризиками, хоча це питання вже давно виходить за межі лише однієї служби. Правильно обліковані та оцінені активи дозволяють ефективно керувати вже наявними вигодами та оцінити потенціал їх використання у майбутньому, а також впливають на інвестиційну привабливість компанії.

У нинішні дні майже у всіх підприємствах вся інформація обробляється за допомогою багаторівневих систем обробки даних, які потенційно несуть загрозу витоку інформації.

Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [1].

За статистикою, визначеною відомою німецькою онлайн-платформою Statista, яка спеціалізується на зборі та візуалізації даних, частка підприємств у всьому світі, які зазнали втрати конфіденційної інформації станом на лютий 2023 року становить 63 % (рис. 1.1.).

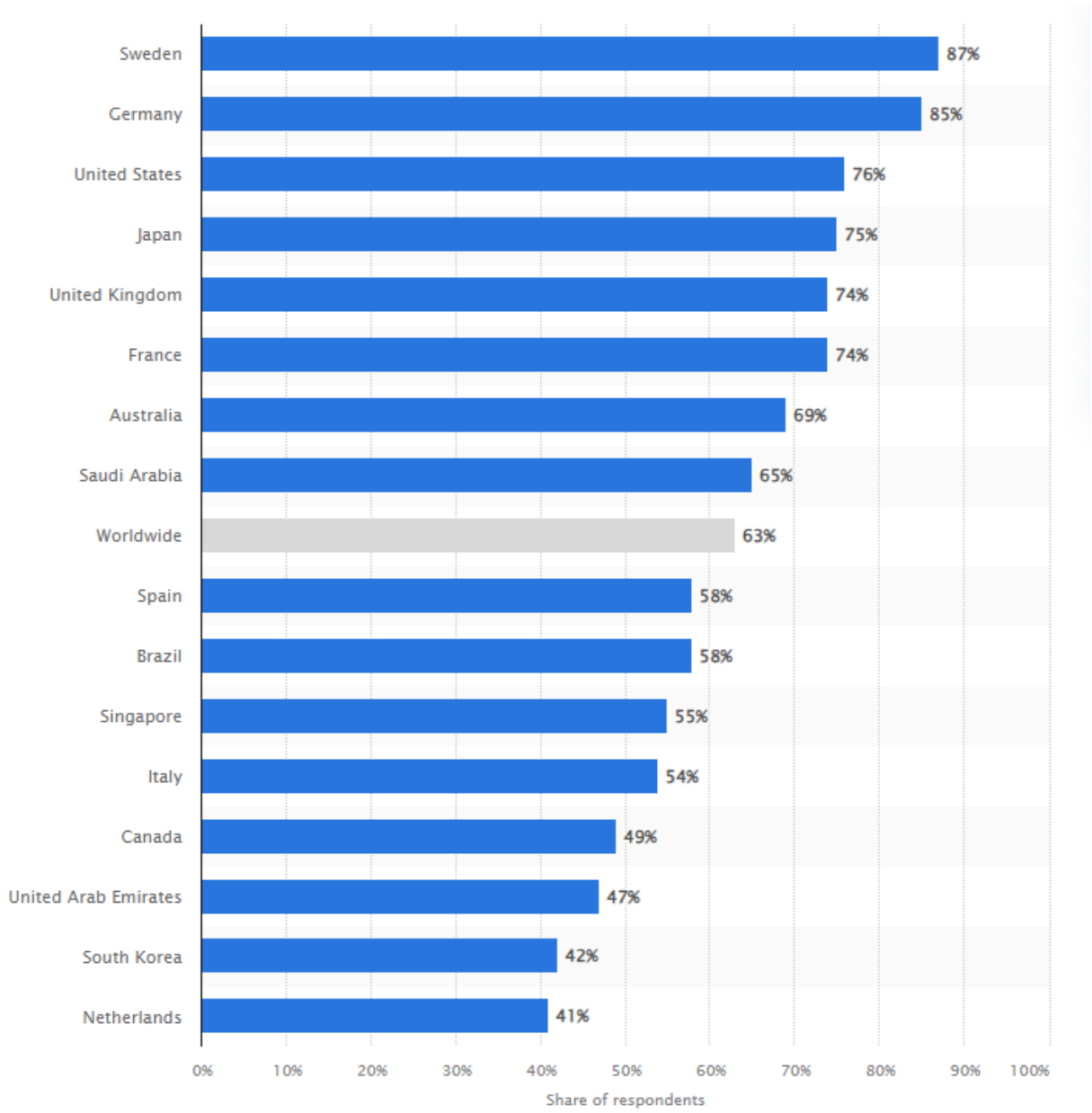


Рис. 1.1. Статистика по країнах щодо втрати конфіденційної інформації

Джерело: складено автором на основі [2]

Виток навіть невеликої частини конфіденційної інформації може призвести до серйозних фінансових втрат та порушення репутації підприємства. Отже, захист інформації стає невідкладним завданням для будь-якого підприємства.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [3].

Основними засобами захисту інформації є:

• фізичні засоби, що необхідні для зовнішнього захисту обчислювальної техніки, території та об'єктів на базі персонального комп'ютера, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та даних, що захищаються;

• апаратні засоби, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв 'язку тощо;

• програмні засоби, що необхідні для виконання логічних і інтелектуальних функцій захисту, які вмонтовані до складу програмного забезпечення системи;

• апаратно-програмні засоби, які широко використовуються при автентифікації користувачів, накладанні електронно-цифрових підписів відповідальних користувачів;

• криптографічні методи, призначені для шифрування або кодування інформації;

• організаційні заходи захисту щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу.

Захист інформації у контексті забезпечення інформаційної безпеки – це сукупність технологій, стандартів, політик та практик управління, які застосовуються до інформації для її збереження.

Система мір по захисту інформації в широкому розумінні повинна бути основана виходячи із початкових умов і факторів, котрі, в свою чергу, визначаються станом спрямованості розвідок противника або діями конкурента

на ринку товарів та послуг, які направлені на захоплення інформації, яка повинна бути захищена [4].

У цілому, захист інформації та правильна оцінка інформаційних активів є критичними завданнями для будь-якого підприємства, оскільки ці активи є основою для успішного функціонування та конкурентоспроможності на ринку. Посилення заходів зі збереження та захисту інформації, а також систематичне оновлення методів її оцінки є ключовими складовими стратегії управління ризиками та забезпечення стійкості бізнесу.

1.2 Канали витоку інформації

Канали витоку інформації існують у будь-якому інформаційному просторі. В загальному розумінні канали витоку інформаці – це передача даних або відомостей за межі певної системи або підприємства неконтрольованим способом. В результаті передачі інформації через канали витоку, зловмисник може отримати несанкціонований доступ до конфіденційної інформації, яку він використає для досягнення своїх цілей.

Канали витоку інформації можна розділити за фізичними властивостями і принципам функціонування [5]:

- акустичні – запис звуку, підслуховування і прослуховування;
- акустоелектричні – отримання інформації через звукові хвилі з подальшою передачею її через мережі електроживлення;
- віброакустичні – сигнали, що виникають за допомогою перетворення інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються;
- оптичні – візуальні методи, фотографування, відеозйомка, спостереження;
- електромагнітні – копіювання полів шляхом зняття індуктивних наводок;

- радіовипромінювання або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом;
- матеріальні – інформація на папері або інших фізичних носіях інформації

Всі канали витоку інформації можна класифікувати на прямі та непрямі. До прямих каналів витоку належать ті, які потребують безпосереднього доступу, як до даних, що обробляються в системі, так і до апаратного забезпечення. А непрямі канали не потребують буквального доступу до інформації.

Передачі інформації через канали вотоку сприяють різноманітні фактори. Вони можуть становити серйозну загрозу для підприємств, порушуючи конфіденційність, цілісність та доступність чутливих даних.

Фактори вотоку можна розділити на наступні групи:

• застосування складних систем обробки інформації. Для підвищення швидкості бізнес-процесі великі компанії створюють великі інформаційно-комунікаційні системи, однак чим складніша система, тим менше вона захищена через притаманну їй складність і масштаб. З більшою кількістю компонентів і точок доступу є більше можливостей для виникнення вразливостей. Крім того, адміністративне навантаження щодо підтримки безпеки у великій системі може бути величезним, що може призвести до недогляду або скоєння прогалин у забезпеченні безпеки. Варто зазначити, що при недостатній захищеності системи, зловмисник може скористатися бекдорами для отримання несанкціонованого доступу до комп’ютера, що знаходиться в цій системі;

• збої при роботі серверів. Збої на сервері можуть спричинити витік даних насамперед через втрату контролю та доступу до збереженої інформації. Проблеми в роботі серверів можуть часто виникати в наслідок хакирських атак або інших непередбачуваних факторів, і коли сервер виходить з ладу, це може призвести до тимчасової або постійної недоступності даних, що робить їх вразливими для несанкціонованого доступу або пошкодження;

• виникнення помилок в роботі ПЗ. Виникнення помилок під час роботи програмного забезпечення може призвести до витоку даних насамперед через уразливості, створені цими помилками. Помилки програмного забезпечення, також відомі як баги, можуть проявлятися в різних формах, наприклад переповнення буфера, логічні недоліки або неправильна перевірка введення. Крім того, використання застарілих версій ПЗ також несе за собою загрозу витоку даних, адже у зловмисників з'являється можливість скористатися різними експлойтами, які часто представляють собою тільки першу частину великої атаки;

• робочий персонал. Всі працівники компанії становлять потенціну загрозу витоку даних. Співробітники, підрядники чи інша частина персоналу, які мають доступ до даних у межах підприємства, можуть навмисно чи ненавмисно спричинити виток даних. Навмисний виток даних спричиняють інсайдери, які керуються власними цілями або працюють на бізнес-конкурентів. Тому підприємства повинні запроваджувати надійні засоби контролю доступу, програми навчання співробітників і механізми моніторингу, щоб зменшити можливість витоку даних таким чином;

• кооперативні об'єднання. Хоча співпраця та партнерство між підприємствами можуть принести численні переваги, зокрема підвищення ефективності та інновацій, однак цей процес є ризиковим. Під час виконання сумісних проєктів з іншим підприємством повною мірою забезпечити захист даних неможливи, оскільки доступ до них має більша кількість людей, що в свою чергу поширює вищевказану групу факторів витоку пов'язану з робочим персоналом;

• переїзди до інших офісних приміщень. Переїзд в інше офісне приміщення представляє потенційну загрозу витоку даних через невід'ємні ризики, пов'язані з фізичним переміщенням і передачею конфіденційної інформації. Під час процесу переміщення існує підвищена ймовірність неправильного розміщення або втрати фізичних документів, пристроїв зберігання чи інших матеріальних активів, що містять конфіденційні дані. Крім того, логістичні проблеми, такі як

пакування, транспортування та розпакування обладнання, можуть збільшити ймовірність провалів у безпеці внаслідок недостатнього догляду. Крім того, залучення сторонніх вантажників або підрядників створює додаткові вразливості, оскільки вони можуть мати доступ до конфіденційної інформації під час процесу переїзду. Таким чином, переїзд в інші офісні приміщення вимагає ретельного планування, оцінки ризиків і впровадження заходів безпеки, щоб мінімізувати ризики витоку даних протягом переїзного періоду.

1.3 Загальні практики забезпечення інформаційної безпеки

Інформаційна безпека – це комплекс заходів, технологій, процесів та політик, спрямованих на захист інформаційних ресурсів підприємства від несанкціонованого доступу, втрати, зміни або знищення. Вона охоплює всі аспекти забезпечення конфіденційності, цілісності та доступності інформації, а також забезпечення безпеки систем і мереж, які цю інформацію обробляють.

Забезпечення інформаційної безпеки на підприємстві є критично важливим завданням, яке вимагає комплексного підходу та впровадження різноманітних практик.

Інформаційна безпека виконує такі важливі функції для підприємства[6]:

− забезпечує безпечну роботу програми, реалізованої в системах інформаційних технологій будь-якого підприємства;

− здійснює захист даних, які підприємство збирає та використовує;

− захищає технологічні активи, що використовуються на підприємстві;

− захищає здатність підприємства функціонувати.

З метою забезпечити інформаційну безпеку, підприємства впроваджують свої стратегії та дотримуються певних загальних практик. Основними практиками захисту є такі:

1. Оцінка та аналіз ризиків інформаційної безпеки

Оцінка та аналіз ризиків інформаційної безпеки включають в себе ідентифікацію потенційних ризиків та можливих наслідків для підприємства.

2. Регулярне проведення аудиту ІБ

Аудит інформаційної безпеки передбачає структуроване обстеження, спрямоване на отримання неупереджених оцінок, як якісних, так і кількісних, щодо поточного стану інформаційної безпеки підприємства. Ця оцінка проводиться відповідно до попередньо визначених критеріїв і показників безпеки.

У загальному вигляді під час проведення аудиту ІБ вирішуються такі завдання [7 с. 20]:

- збір та аналіз первинних даних про підприємство та його функціональну структури ІКС, необхідних для оцінки стану ІБ;

- аналіз існуючої політики забезпечення ІБ на предмет повноти та ефективності;

- аналіз інформаційних і технологічних ризиків, пов'язаних із реалізацією загроз ІБ;

- тестові спроби несанкціонованого доступу до критично важливих вузлів ІКС та визначення уразливості в налаштуваннях захисту цих вузлів;

- формування рекомендацій з розробки (або доопрацювання) політики забезпечення інформаційної безпеки на підставі аналізу існуючого режиму інформаційної безпеки;

- формування пропозицій щодо використання існуючих та встановлення додаткових засобів захисту інформації для підвищення рівня надійності та безпеки ІКС підприємства.

3. Створення та періодичне оновлення політики безпеки

Створення та періодичне оновлення політики безпеки має першочергове значення для будь-якого підприємства, незалежно від його розміру чи галузі. Політика безпеки по суті є фундаментом, на якому будується конструкція захисту активів підприємства і забезпечення конфіденційності, цілісності та доступності її інформації.

Політика безпеки складається з певних положень, які визначають різні правила щодо використання паролів, контролю доступу, обміну даними і тому подібне.

4. Створення резервних копій і розробка плану відновлення.

Втрата даних може статися через різні фактори, такі, як збій апаратного забезпечення, програмні збої, людські помилки, кібератаки або стихійні лиха, тому розробка плану відновлення є критично важливою для будь-якого підприємства. Віддповідно до плану відновлення та політики безпеки регулярно проводиться резервне копіювання даних.

Резервне копіювання або бекап – створення копій всіх файлів, наявних на пристрої, жорсткого диска на інших пристроях або передача їх для зберігання в хмарі на випадок втрати або пошкодження комп'ютера. Резервне копіювання даних необхідно виконувати з тією частотою, з якою відбувається оновлення документів [8].

5. Шифрування критично важливих даних.

Шифрування даних є ще однією важливою складовою захисту конфіденційної інформації підприємства. Тому слід регулярно оцінювати класифікацію даних і застосовувати шифрування за необхідності. Використання VPN (Virtual Private Network) може забезпечити ще один рівень захисту для співробітників, яким, можливо, доведеться отримати доступ до конфіденційних файлів з віддалених місць.

6. Регулярне оновлення програмного забезпечення

Своєчасне оновлення ПЗ надає можливість використовувати найбільш актуальну версію, що теоретично містить менше вразливостей. До того ж, оновлення програмного забезпечення вводять нові функції, покращення та оптимізацію, які поліпшують продуктивність, зручність використання та сумісність.

7. Використання технологій контролю доступу та додавання багатофакторної автентифікації

Використовуючи технології контролю доступу, адміністрація застосовує обмеження для користувачів відповідно до призначених ролей. На практиці часто використовується PAM (Privileged Access Management) для виявлення та запобігання несанкціонованому привілейованому доступу до критично важливих ресурсів.

Багатофакторна автентифікація — це розширена перевірка належності акаунта користувачеві, що включає більше одного фактора. Під факторами мають на увазі [9]:

- фактор знання – інформація, відома суб'єкту – ПІН-код, пароль, контрольне слово, відповідь на секретне запитання;
- фактор володіння – річ, що належить користувачеві – телефон, телефон, планшет, персональний комп'ютер, токен безпеки, смарт-картка;
- фактор властивості – біологічні характеристики суб'єкта – відбиток пальця або долоні, райдужка ока, голос, обличчя.

Додавання багатофакторної автентифікації забезпечує більш надійний захист, адже зловмисникові буде важко отримати несанкціонований доступ навіть тоді, коли один із факторів стає доступний йому.

8. Навчання та перевірка обізнаності персоналу

Навчання та перевірка обізнаності персоналу є не менш важливими складовими безпеки на підприємстві. Всі працівники, які є користувачами ІКС, повинні бути ознайомлені з політиками та процедурами безпеки, а також мати необхідні навички щодо запобігання певних ризиків безпеки. Регулярні тренування для підвищення обізнаності та тестування для закріплення знань гарантують, що персонал підприємства завжди буде готовий відреагувати на нові виклики і загрози.

9. Постійне обслуговування інфраструктури безпеки

Постійне обслуговування інфраструктури безпеки є критично важливим компонентом забезпечення кібербезпеки підприємства. Це передбачає регулярне моніторинг, оновлення, вдосконалення та тестування систем та процесів, щоб забезпечити їх надійність і стійкість до нових загроз.

10. Впровадження DLP-системи

Система запобігання витокам даних – це сукупність технологій та процесів, спрямованих на захист конфіденційної інформації від несанкціонованого доступу, передачі або втрати. Впровадження DLP є важливою частиною стратегії інформаційної безпеки підприємства.

Висновки до розділу 1

Витік конфіденційної інформації є серйозною загрозою для безпеки даних у сучасному світі. Проблема виникає з різних джерел, включаючи недбалість співробітників, використання незахищених інструментів обміну інформацією та активності зловмисників, таких як фішингові шахрайства. Попередження витоку інформації вимагає комплексного підходу, що включає в себе технічні заходи безпеки, освіту персоналу та розробку стратегій протидії кіберзлочинності. Шляхом посилення заходів захисту даних та удосконалення процесів безпеки можна мінімізувати ризики витоку інформації та забезпечити збереження конфіденційності та цілісності даних.

Підприємства, які приділяють належну увагу захисту даних, мають більші шанси уникнути негативних наслідків витоку інформації, таких, як втрати фінансових та репутаційних ресурсів, порушення законодавства щодо захисту персональних даних та втрата довіри клієнтів і партнерів. Тому висока увага до захисту інформації має бути однією з основних пріоритетних завдань для будь-якого підприємства чи установи.

Розділ 2 АНАЛІЗ ВИКОРИСТАННЯ DLP-СИСТЕМ

2.1 Загальні відомості про DLP-системи

DLP-система (Data Loss / Leak Prevention) являє собою комплекс інструментів та процесів, спрямованих на виявлення та запобігання несанкціонованому використанню, втраті або витоку конфіденційної інформації на підприємстві. Ці системи застосовують різні методи для захисту корпоративної мережі, включаючи виявлення, класифікацію, моніторинг та блокування даних у разі потреби.

Така система створює захищений «цифровий периметр» навколо підприємства, аналізуючи всю вхідну, вихідну і внутрішню інформацію. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифу документа, спеціально введених міток, значень хеш-функції тощо.

Основними завданнями DLP-систем є:

– формалізація опису даних, які підлягають захисту, відповідно до параметрів налаштування системи;

– виявлення конфіденційної інформації у потоці вихідних даних з внутрішньої інформаційної мережі компанії, включаючи аналіз дій, спрямованих на переміщення цих даних;

– реагування на виявлені спроби витоку даних та створення доказової бази для подальшого розслідування інцидентів;

– визначення потенційних ризиків і загроз, що стосуються конфіденційної інформації;

– забезпечення відповідності до регуляторних вимог, включаючи вимоги щодо захисту даних;

– моніторинг та аналіз дій користувачів для забезпечення безпеки даних.

Основні функції DLP-систем включають:

- контроль передачі інформації через Інтернет з використанням різних протоколів і додатків, таких як e-mail, http, https, ftp тощо;
- моніторинг збереження інформації на зовнішніх носіях та мобільних пристроях;
- захист інформації від витоку шляхом контролю друку даних;
- блокування спроб пересилання або збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, спроби створення копій;
- пошук конфіденційної інформації на робочих станціях і файлових серверах за ключовими словами, мітками документів, атрибутами файлів і цифровими відбитками;
- запобігання витоку інформації шляхом контролю життєвого циклу і руху конфіденційних відомостей.

Використання DLP-систем може розв'язати такі питання:

– запобігання витокам і несанкціонованій передачі конфіденційної інформації;

– мінімізація ризиків фінансових і репутаційних втрат;

– підвищення дисципліни користувачів;

– розслідування інцидентів та їх наслідків;

– ліквідація загроз безпеки персональних даних і відповідність вимогам щодо захисту персональних даних.

Дані можуть перебувати в трьох різних станах (рис. 2.1.), розуміння яких допоможе обрати правильні заходи для забезпечення їх захисту [10]:

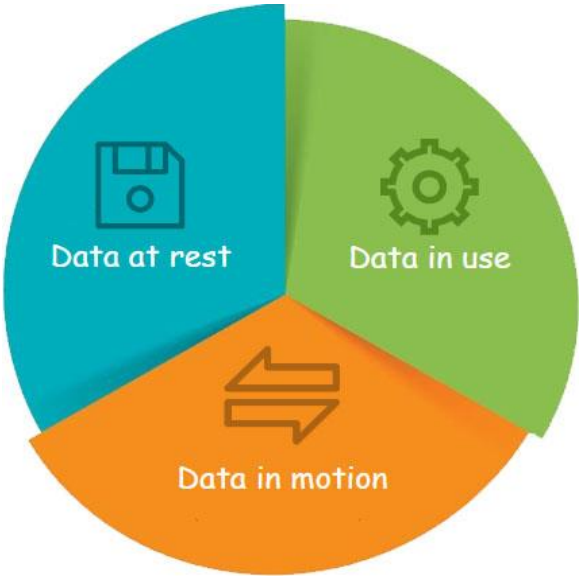


Рис. 2.1. Стани даних

1) Data In Motion (Дані у русі) – дані, які передаються з одного місця зберігання в інше. Прикладом цього може вважатися переміщення файлу з одного жорсткого диска на інший або електронний лист, що надсилається через мережу Інтернет.

2) Data In Use (Дані у використанні) – дані, які активно використовуються будь-яким програмним забезпеченням.

3) Data At Rest (Дані у спокої) – дані, які зберігаються на жорсткому диску і не передаються або не використовуються зараз. Їх ще називають пасивними даними.

Варто звернути увагу на те, що деякі DLP-системи можуть захищати лише дані, які перебувають у певному конкретному стані, і це є важливим аспектом при виборі DLP-рішення для подальшого впровадження.

Більшість DLP-систем працюють на основі політик, які встановлюються адміністратором. Ці політики містять певні правила для мережі або кінцевих пристроїв, чітко визначаючи дозволені та заборонені дії. Політики можуть бути загальними або стосуватися конкретних програм, веб-сторінок або кінцевих пристроїв. Також адміністратори можуть налаштовувати політики для контролю

користувачів, що мають різні рівні доступу відповідно до своїх ролей. Чим більш докладно та специфічно налаштовані політики, тим менше помилок виникає у роботі DLP-системи, що сприяє підвищенню її ефективності.

Останнім часом, вимоги до можливостей DLP-систем постійно зростають, що перетворює їх у одні з найбільш ефективних, комплексних та системних рішень у сфері захисту конфіденційної корпоративної інформації.

Сучасна DLP-система представляє собою розподілений програмно-апаратний комплекс, який складається з декількох модулів. Кожен з модулів DLP-системи відповідає за вирішення своєї специфічної задачі з метою забезпечення повноцінного контролю та захисту конфіденційної інформації на підприємстві. Ці модулі є важливими компонентами системи та працюють спільно для забезпечення ефективної захисту даних. Вони дозволяють адміністраторам системи та іншим зацікавленим сторонам моніторити, аналізувати та реагувати на різноманітні аспекти використання даних на підприємстві, що допомагає у запобіганні витокам інформації та іншим загрозам безпеці.

Модулі DLP-системи функціонують на окремих серверах, на робочих місцях співробітників компанії (таких як персональні комп'ютери, робочі станції та інші пристрої) і на рівні внутрішньої служби безпеки. Цей комплекс включає в себе:

- Модулі бази даних, систематизації, аналізу та обробки інформації, які стосуються всіх інцидентів, виявлених системою, а також іншої інформації, що включена до системи відстеження та контролю.
- Модулі пасивного чи активного спостереження, які відслідковують та контролюють дії співробітників компанії. Ці модулі моніторять різні дії, включаючи вхід та вихід з системи, бездротову передачу даних, підключення зовнішніх пристроїв, друк документів та інші процеси.
- Модулі управління, моніторингу та налаштування системи, які використовуються для адміністрування системи та аналізу даних для потреб служби безпеки.

Кожен з модулів DLP-системи відповідає за вирішення своєї специфічної задачі. Тому варто розглянути головні функціональні модулі, з яких може складатися DLP-система (рис. 2.2.).

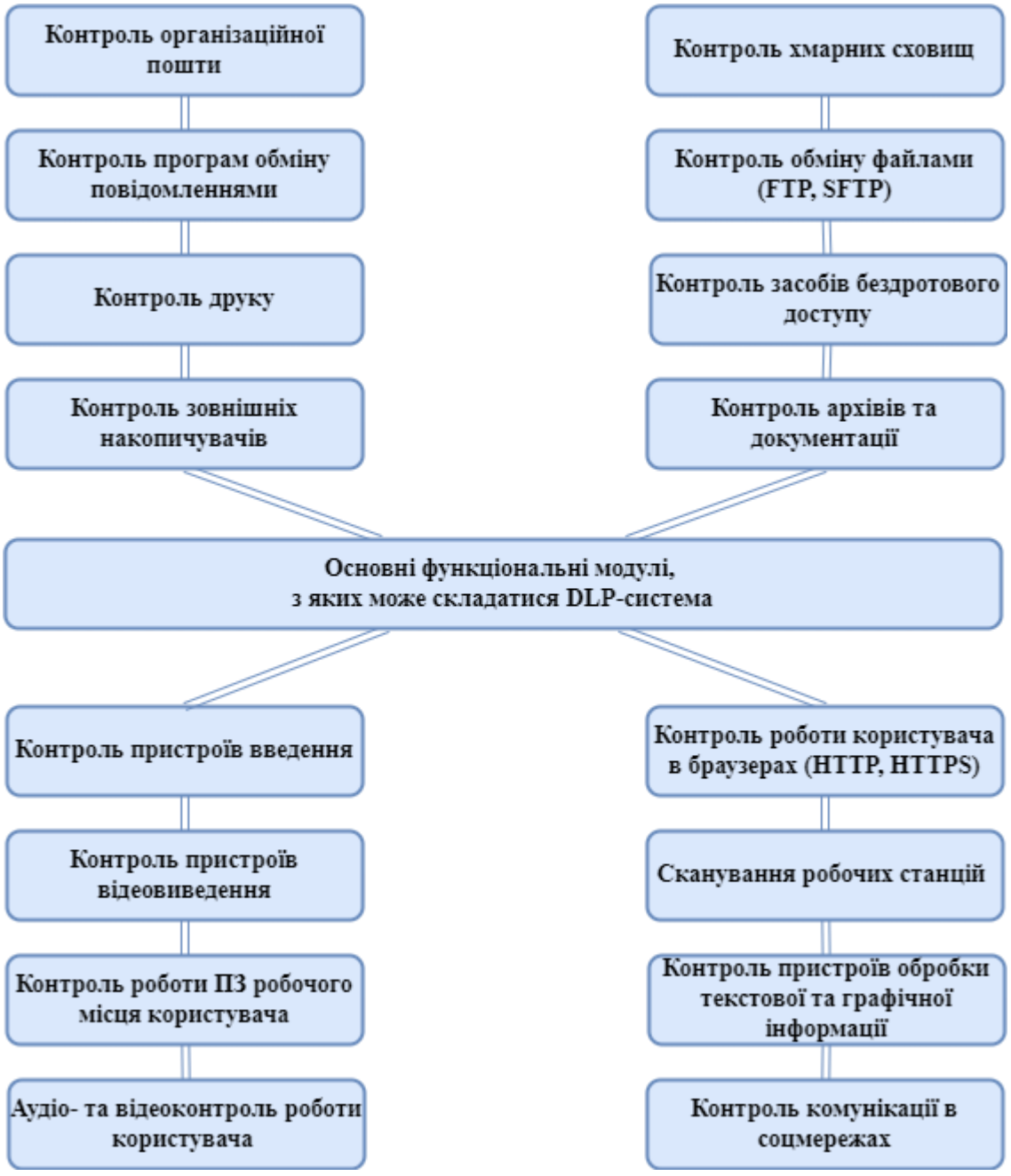


Рис. 2.2. Основні функціональні модулі DLP-системи

Для аналізу даних DLP-система має їх одержати у вигляді потоків інформації з різних джерел. Для цього використовуються два основні способи

перехоплення інформації – серверний та агентський. У першому випадку система контролює трафік на сервері, через який комп'ютери взаємодіють із зовнішньою мережею. У другому випадку спеціальні невеликі програми (агенти) – встановлюються на всі комп'ютери підприємства та передають з них дані для аналізу.

Агентське перехоплення є більш поширеним, адже з його допомогою можна отримати набагато більше даних із різних каналів, а значить краще запобігти можливим витокам.

DLP-система може працювати тільки в двох режимах – активному або пасивному. Кожен з режимів має свої переваги та недоліки. Вибір конкретного режиму залежить від потреб та унікальних вимог підприємства.

У активному режимі роботи система DLP може миттєво реагувати на виявлені інциденти шляхом блокування трафіку, що запобігає потенційним витокам інформації. Цей режим дозволяє системі самостійно сканувати трафік і вживати відповідні заходи у разі виявлення порушень згідно з налаштованими політиками безпеки. Однак головним недоліком активного режиму є можливість виникнення помилкового сигналу про порушення безпеки, що може спричинити призупинення підприємницької діяльності. Цей феномен, відомий як False-positive спрацювання, може виникати в результаті недостатньо точної калібровки системи.

У пасивному режимі роботи система DLP здійснює моніторинг трафіку без його блокування. Зазвичай це виконується за допомогою окремого пристрою, який аналізує зеркальне відображення трафіку (SPAN) з метою виявлення потенційних порушень безпеки. Хоча в пасивному режимі система не може блокувати трафік, вона збирає дані для подальшого аналізу та формування звітів. Адміністратор в змозі виявити виток конфіденційної інформації та донести про інцидент до керівництва, але система не втручається у процес передачі даних.
Пасивний режим може спільно працювати з іншими технологіями, такими як SIEM, що допомагає адміністраторам здійснювати більш комплексний аналіз та реагування на загрози безпеки.

2.2 Види DLP-систем і принципи їх функціонування

Існують різні види DLP-систем, кожна з яких має свої унікальні характеристики та функціональні можливості. Залежно від потреб та специфіки підприємства, вибір підходящої DLP-системи може бути критичним для забезпечення ефективного контролю за безпекою даних та управління ризиками.

Існують такі види DLP-систем:

- Мережеві
- Хмарні
- Захист кінцевих точок

Варто зазначити, що також існують DLP з малим функціоналом, які призначені тільки для захисту електронної пошти, що являє собою програмне забезпечення, яке відстежує лише електронні листи, надіслані користувачам в межах підприємства.

Мережева DLP-система – це життєво важливе рішення безпеки, яке відстежує передачу даних у мережі компанії. Її основна мета – захистити дані від небажаного доступу та витоку під час передачі між кінцевими точками мережі. Вона гарантує, що дані, які передаються через мережу підприємства, не будуть перехоплені або доступні без авторизації. Це запобігає витоку даних і забезпечує конфіденційність інформації під час передачі, суворо дотримуючись вимог захисту даних. Мережева DLP-система також здатна виявляти та запобігати внутрішнім загрозам, таким чином захищаючи критичну інформацію.

Схему розгортання мережевої DLP-системи наведено на рис. 2.3.

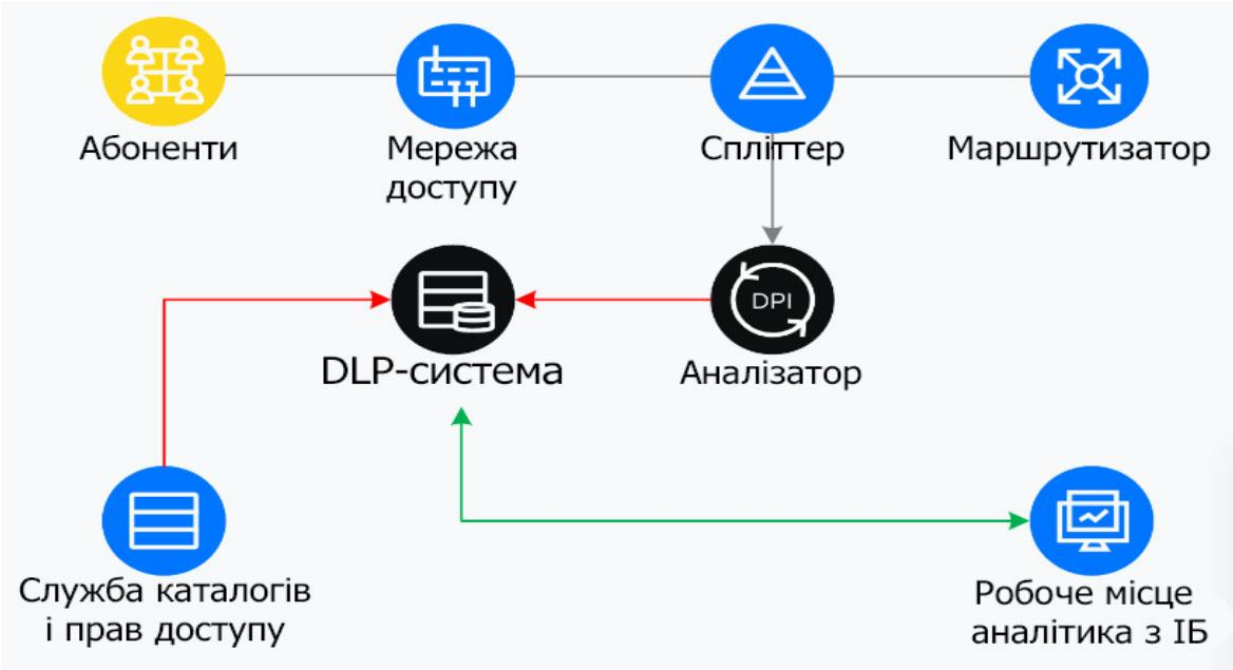


Рис. 2.3. Схема розгортання мережевої DLP-системи

Хмарна DLP-система – це потужне рішення, яке захищає дані, що зберігаються та обробляються в хмарних середовищах, включаючи програми SaaS, хмарні служби зберігання та хмарні бази даних. Вона є цінним інструментом для підтримки контролю над конфіденційними даними та запобігання потенційним витокам під час співпраці та обміну файлами в хмарі. Захищаючи дані в різних хмарних програмах, хмарна DLP-система забезпечує відповідність нормативним вимогам. Вона розширює безпеку даних за межі мережі вашого підприємства, що робить її незамінним інструментом для компаній з віддаленими співробітниками та географічно розосередженими операціями.

Процес роботи хмарної DLP-системи наведено на рис. 2.4.

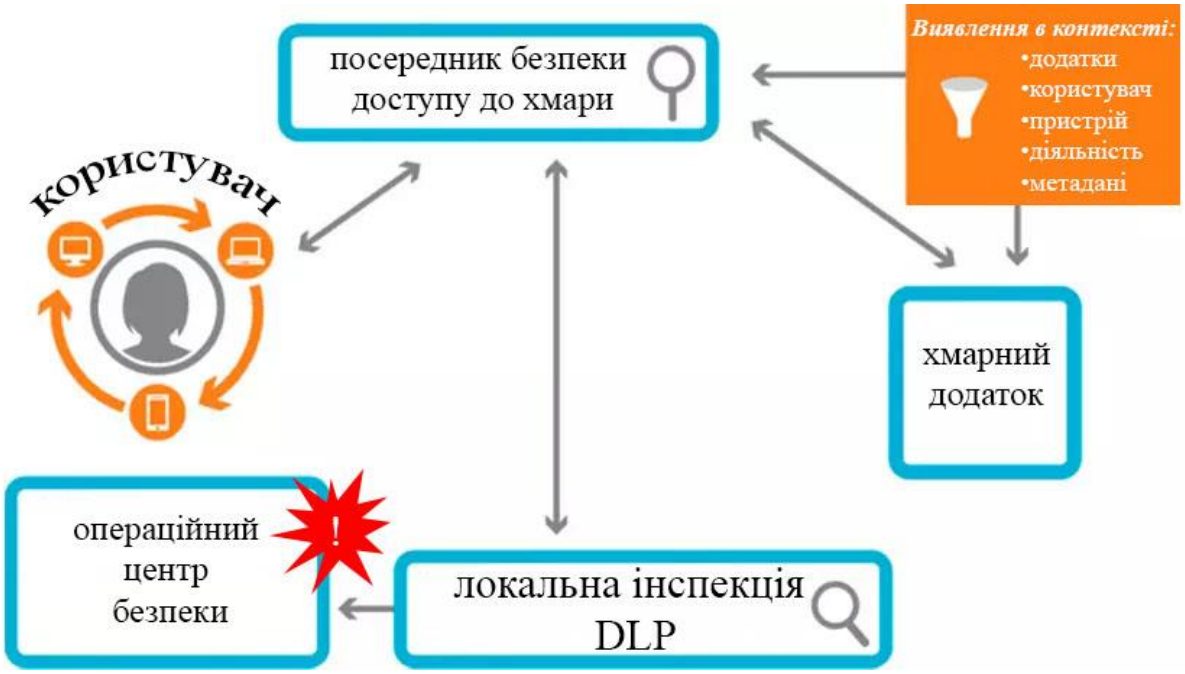


Рис. 2.4. Процес роботи хмарної DLP-системи

DLP-система кінцевих точок захищає важливі дані на окремих пристроях і кінцевих точках, таких як ноутбуки, мобільні телефони та планшети. У сучасних віддалених робочих середовищах співробітники часто використовують пристрої за межами корпоративної мережі для доступу до даних. Завдяки Endpoint DLP можна бути впевненими, що конфіденційна інформація знаходиться в безпеці на цих пристроях. DLP-система кінцевих точок також допомагає запобігти крадіжці даних через знімні носії, такі, як USB-накопичувачі, та захищає від несанкціонованої передачі даних через електронну пошту або хмарні служби на пристроях співробітників. Вона особливо важлива для підприємств, які мають справу з конфіденційною інформацією, проводять дослідження або працюють з чутливими документами. DLP-система кінцевих точок захищає інтелектуальну власність, забезпечуючи конфіденційність даних.

Порівняння різних видів DLP наведено в табл. 2.1.

Таблиця 2.1.

Порівняння різних видів DLP

Параметри	**Мережева DLP-системи**	**Хмарна DLP-системи**	**DLP-система кінцевих точок**
Область застосування	Відстежує дані, що передаються в мережі Наприклад: електронні листи, веб-трафік і обмін файлами	Відстежує дані, що передаються та зберігаються в програмах SaaS і хмарних середовищах Наприклад: Slack, Google Workspace, Dropbox, AWS або Azure	Відстежує дані на окремих пристроях і кінцевих точках Наприклад: ноутбуки, смартфони, планшети та USB-накопичувачі
Захист даних	Захищає інформацію від несанкціонованого доступу та злому в межах корпоративної мережі	Забезпечує безпеку як збережених, так і переданих даних у SaaS і хмарних середовищах. Захищає конфіденційну інформацію під час використання будь-яких програм SaaS або Cloud	Мінімізує ризик втрати даних у разі крадіжки пристрою або незаконного доступу, захищаючи дані на ноутбуках та інших пристроях за межами мережі підприємства. Сприяє конфіденційності даних і захищає інтелектуальну власність
Розгортання	Встановлюється на мережевому шлюзі для перевірки та фільтрації пакетів у реальному часі	Інтеграція на основі API або проксі-сервера з хмарними платформами або хмарними службами зберігання для відстеження доступу до даних і активності	Встановлюються як програмні агенти або програми на певних пристроях або кінцевих точках для локальної реалізації протоколів безпеки
Масштабованість	Може бути складною для масштабування, оскільки це може включати значні зміни в апаратному та програмному забезпеченні	Легко масштабується зі зростанням використання хмари, забезпечуючи гнучкість у міру зміни потреб	Масштабується, але може знадобитися надійна система керування пристроєм для забезпечення узгодженого застосування на всіх пристроях.

Продовження таблиці 2.1.

Налаштування	Може знадобитися ретельне налаштування, щоб збалансувати захист і зручність використання. Неможливо сканувати вкладення або складні неструктуровані документи	Пропонує налаштований контроль за допомогою SaaS і хмарних додатків, адаптованих до конкретних програм і типів даних (включаючи документи всіх типів - pdf, jpeg, зображення, знімки екрана, аудіофайли, документи Word, електронні таблиці Excel тощо)	Менша точність для складних даних
Технічне обслуговування	Для забезпечення ефективності системи потрібні регулярні оновлення, налаштування та моніторинг	Легко обслуговувати, оскільки ним керують постачальники SaaS/Cloud DLP, що зменшує навантаження на обслуговування	Впровадження та обслуговування є дорогими, складними та трудомісткими
Переваги	Захищає дані від злому та несанкціонованого доступу	Забезпечує централізоване керування та безпеку даних, що зберігаються в хмарі	Забезпечує безпеку даних за межами корпоративної мережі
Виклики	Проблеми включають складність налаштування і потенційну високу вартість	Залежність від хмарного постачальника може призвести до потенційної затримки або проблем із сумісністю	Управління кількома кінцевими точками, забезпечення узгодженості та керування віддаленими пристроями може бути складним

Підсумовуючи, вибір відповідної DLP-системи залежить від конкретних потреб і операційного контексту підприємства. Кожен тип пропонує певні переваги та відіграє вирішальну роль у комплексній стратегії безпеки даних. Ефективно запровадивши правильне рішення DLP, підприємства можуть значно підвищити рівень кібербезпеки та зменшити ризики витоку даних.

2.3 Методи виявлення конфіденційної інформації

Один із найпростіших методів контролю – це сигнатурний метод, який базується на пошуку в потоці даних певної послідовності символів. Заборонену послідовність символів іноді називають «стоп-виразом», але загалом це може бути довільний набір символів, наприклад, певна мітка. Якщо система налаштована на пошук одного слова, то результат її роботи – визначення 100% збігу, що робить цей метод детерміністичним. Проте, частіше пошук певної послідовності символів застосовується при аналізі тексту. У більшості випадків сигнатурні системи налаштовані на пошук кількох слів та визначення частоти їхнього використання.

До переваг сигнатурного методу відноситься простота поповнення словника заборонених термінів, очевидність принципу роботи, а також висока надійність у випадках, коли необхідно знайти точну відповідність слова чи виразу.

Недоліки стають очевидними під час промислового використання цієї технології для виявлення витоків і налаштування правил фільтрації. Більшість виробників DLP-систем орієнтовані на західні ринки, де англійська мова має «сигнатурний» характер – форми слів зазвичай утворюються за допомогою прийменників без зміни самого слова. В українській мові, наприклад, ситуація складніша через наявність префіксів, суфіксів, закінчень. Наприклад, слово «ключ» може мати значення як «ключ шифрування», «ключ від квартири», «джерело», «ключ або PIN-код від кредитної картки», та багато інших. В українській мові з кореня «ключ» можна утворити десятки різних слів.

Ще один метод, відомий як "цифрові відбитки", використовує різні типи хеш-функцій для визначення унікальних характеристик конфіденційних документів. Цей підхід представляється західними розробниками DLP-систем як новаторський на ринку захисту від витоків, хоча сама технологія існує з 70-х років. Основна ідея втілення цього методу є однаковою, але конкретні алгоритми можуть відрізнятися від виробника до виробника.

Суть роботи "цифрових відбитків" досить проста і приваблива: стандартний документ-шаблон надсилається DLP-системі, з якого генерується "цифровий відбиток" і записується в базу даних. Після цього в правилах контентної фільтрації настроюється відсоткова відповідність шаблону з базою.

Наприклад, якщо налаштувати 70% відповідність "цифрового відбитка" до договору поставки, то DLP зможе виявити практично всі договори цього типу. Іноді цю технологію порівнюють з "антиплагіатом", але остання працює тільки з текстовою інформацією, тоді як "цифрові відбитки" можуть застосовуватися до різноманітного медійного контенту для захисту авторських прав та виконання нормативних вимог інформаційної безпеки.

До переваг "цифрових відбитків" можна віднести простоту додавання нових шаблонів, високий рівень детектування та прозорість алгоритму для співробітників відділів інформаційної безпеки. Недоліком є необхідність постійного оновлення бази даних "цифрових відбитків". Ця технологія, хоч і ефективна, але вимагає значних ресурсів для пошуку та індексації нових і змінених файлів, що може бути складним завданням, особливо для великих компаній. Також важливо враховувати, що низькорівневі хеш-функції, такі як "цифрові відбитки", не стійкі до простого кодування, що може стати проблемою в деяких випадках. Окрім того, збільшення обсягу бази "цифрових відбитків" може призвести до додаткових витрат на зберігання і обробку даних, а також на підтримку продуктивності серверів DLP.

Основним недоліком є те, що, не звиртаючи увагу на простоту і відсутність лінгвістичних методів, потрібно регулярно оновлювати базу даних «цифрових відбитків». І, незважаючи на всі переваги, ця технологія може бути менш ефективною для великих компаній зі значним потоком документів, оскільки вона потребує постійного оновлення та індексації файлів в режимі реального часу.

Також в DLP-системах часто використовується метод "мітки", що передбачає вбудовування спеціальних ідентифікаторів всередині файлів, що містять конфіденційну інформацію. Цей метод забезпечує стабільні та досить точні дані для роботи DLP-системи, але вимагає значних змін в мережевій

інфраструктурі. Водночас, лідери ринку DLP зазвичай не використовують цей метод, тому докладне розглядання його реалізації не має великого сенсу. Варто відзначити, що, незважаючи на очевидні переваги "міток", якість детектування, цей метод також має значну кількість недоліків. Від відсутності систематизації всередині мережі до необхідності встановлення багатьох нових правил і форматів файлів для користувачів. Зрештою, впровадження цієї технології може перетворитися на впровадження спрощеної системи обігу документів.

Для детектування конфіденційної інформації іноді використовуються такі методи, як:

- Лінгвістичний
- Ручне детектування
- Регулярні вирази

Лінгвістичний метод базується на аналізі мовних особливостей тексту для виявлення конфіденційної інформації. Він використовує різноманітні техніки, такі як морфологічний аналіз і стемінг, для перетворення слів у їх базові форми та виявлення відповідностей до певних шаблонів або ключових слів. Наприклад, в англійській мові слово "running" може бути перетворено на базову форму "run" за допомогою стемінгу, що дозволяє виявити усі відповідні форми слова незалежно від їх спряження чи відмінювання.

Лінгвістичний метод є досить ефективним, оскільки він дозволяє враховувати семантичні та граматичні особливості мови. Проте він може бути більш складним у використанні для мов зі складною морфологією, таких як слов'янські мови, де велика кількість спряжень та відмінювань ускладнює процес аналізу. Також, потрібно враховувати, що мовні відмінності можуть впливати на результати, і метод може потребувати постійного оновлення для адаптації до нових лінгвістичних особливостей.

Ручне детектування, також відоме як метод карантину, передбачає ручний аналіз та перевірку конфіденційних даних або файлів і їх відокремлення для подальшого розгляду адміністратором системи. Цей метод часто застосовується для виявлення аномальної або підозрілої активності, яка не може бути ефективно

виявлена за допомогою автоматизованих методів, або для перевірки результатів автоматизованих процесів.

Хоча ручне детектування може бути дуже ефективним у виявленні складних аномалій та нових загроз, воно вимагає значних людських ресурсів та часу. Крім того, цей метод може піддаватися суб'єктивному впливу, оскільки рішення про класифікацію даних може залежати від індивідуальних оцінок та досвіду аналітика. Також, ручне детектування може бути повільним та неефективним для обробки великих обсягів даних.

Метод «регулярні вирази» (Regex) використовуються для пошуку текстових шаблонів у даних або файлових потоках. Цей метод базується на використанні спеціальних виразів, які визначають певні правила пошуку тексту. Регулярні вирази дозволяють виявляти ключові слова, фрази, або шаблони символів, що відповідають конкретним критеріям.

Основною перевагою використання регулярних виразів є їх гнучкість та можливість використання складних шаблонів для пошуку тексту. Вони дозволяють створювати широкий спектр умов для визначення конфіденційної інформації, що робить їх ефективними для виявлення різноманітних загроз та аномалій у данних.

Проте важливо враховувати, що складність регулярних виразів може бути викликана їх складністю та заплутаністю, особливо при роботі з великими обсягами даних. Написання та тестування складних регулярних виразів може вимагати значних зусиль та часу. Крім того, помилки у виразах можуть призводити до неточностей у виявленні конфіденційної інформації, що може вплинути на ефективність системи.

Висновки до розділу 2

Різні види DLP-систем, такі, як мережеві, хмарні та для захисту кінцевих точок, являють собою комплексні рішення, що забезпечують надійний захист конфіденційної інформації в різних середовищах.

Кожна DLP-система використовує певні методи ідентифікації конфіденційної інформації, до них належать: сигнатурний метод, цифрові відбитки, мітки, лінгвістичний аналіз, регулярні вирази та ручне детектування. Кожен з цих методів має свої переваги та недоліки, що дозволяє забезпечувати різні рівні точності та ефективності виявлення загроз.

Ефективне функціонування DLP-систем залежить від комплексного підходу до захисту конфіденційної інформації, що включає використання різних типів систем та методів ідентифікації загроз. Оптимальна комбінація технологій дозволяє забезпечити всебічний захист корпоративних даних, знизити ризики витоку інформації та підвищити загальний рівень безпеки підприємства.

Розділ 3 ОЦІНКА ТА УДОСКОНАЛЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

3.1 Порівняльний аналіз сучасних DLP-систем

За останні роки ринок інструментів DLP суттєво зріс. Зі збільшенням частоти та складності кіберзагроз компанії інвестують більше в рішення DLP, щоб зміцнити свою позицію кібербезпеки.

Попит на популярні DLP-рішення зростає з кожним днем. Ці рішення пропонують багатогранний підхід до захисту конфіденційних даних, охоплюючи такі можливості, як виявлення, класифікація, моніторинг та реагування на інциденти.

На сьогоднішній день популярними DLP-рішенями є такі:

- Forcepoint
- Symantec
- Proofpoint
- Trellix (McAfee)
- Endpoint Protector (CoSoSys)

Forcepoint – це інноваційний інструмент для захисту даних, який пропонує індивідуальний та адаптивний підхід до забезпечення безпеки інформації. Ця система розроблена для захисту даних як у локальних мережах, так і в хмарних середовищах, забезпечуючи надійний захист у будь-яких умовах.

Forcepoint DLP перевершує інші засоби запобігання втраті даних, захищаючи дані скрізь, де користувачі отримують до них доступ [11].

Forcepoint DLP володіє широким спектром функцій, що дозволяють ефективно виявляти, класифікувати, захищати та моніторити дані без впливу на користувацький досвід.

За допомогою Forcepoint можна захистити PII, PCI, PHI (Protected Health Information) та інші конфіденційні дані.

Серед основних характеристик можна виокремити:

• Захист даних у різних форматах. Forcepoint DLP забезпечує захист не тільки структурованих, а й неструктурованих даних, включаючи зображення, креслення, а також фінансові дані та особисту інформацію.

• Відповідність нормативним вимогам. Система працює відповідно до нормативних вимог у понад 80 країнах, включаючи GDPR, PCI NIS 2 (Payment Card Industry Network Information Security 2), HIPAA, CCPA (California Consumer Privacy Act), завдяки широкому набору попередньо визначених шаблонів політик і понад 1700 класифікаторів даних.

• Реагування на інциденти в реальному часі. Forcepoint DLP надає можливість отримувати повідомлення про потенційні порушення даних в режимі реального часу та реагувати на них негайно, що дозволяє запобігти виникненню серйозних інцидентів без зволікань.

Інтерфейс Forcepoint DLP наведено на рис. 3.1.

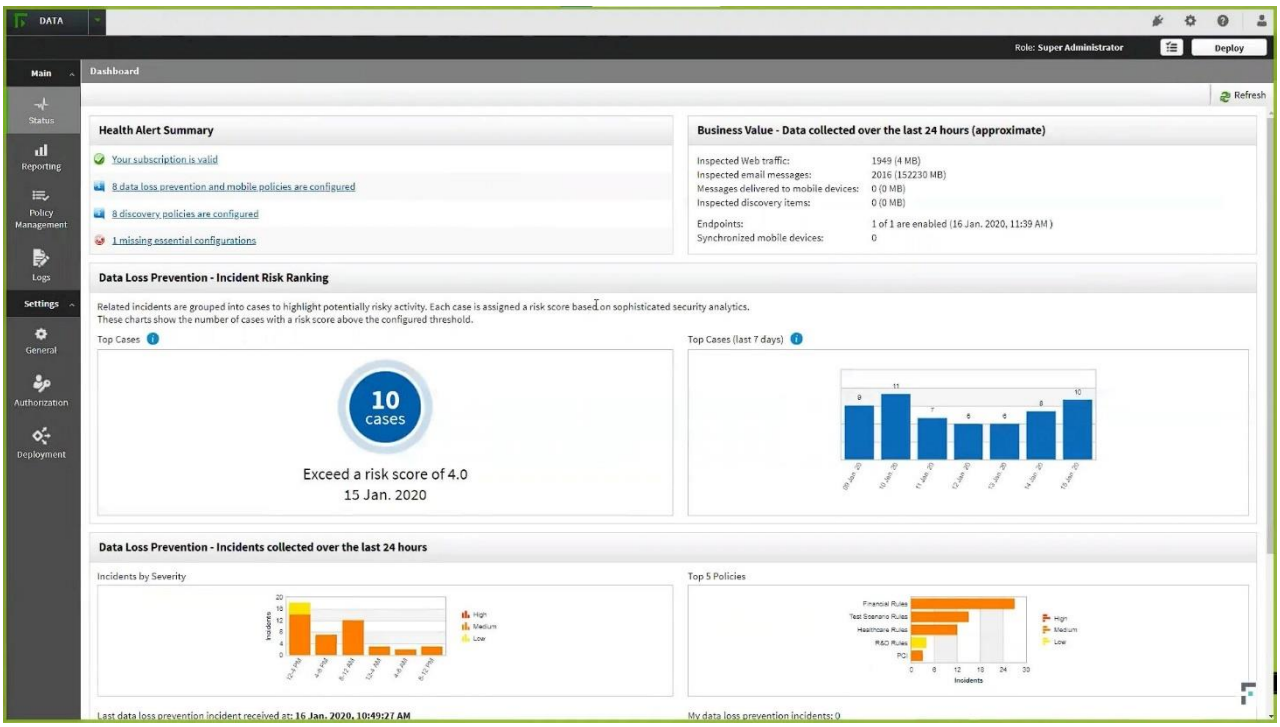


Рис. 3.1. Інтерфейс Forcepoint DLP

Symantec DLP – це комплексне рішення, яке поєднує в собі відстеження активності користувачів з контролем ризику даних. Ця система пропонує рішення для захисту даних для кінцевих точок, мереж, хмарних ресурсів і файлових серверів із центральної консолі. Встановлюється на Windows Server і Linux [12].

Symantec DLP володіє рядом ключових характеристик, які дозволяють ефективно контролювати та захищати дані:

• Відстеження активності користувачів. Система реєструє весь доступ до конфіденційних даних і відстежує облікові записи, що викликали сповіщення, надаючи повну видимість та контроль над даними.

• Захист шифрування. Конфіденційні документи зашифровані, щоб їх могли побачити лише авторизовані користувачі, забезпечуючи додатковий рівень безпеки.

• Відповідність стандартам. Symantec DLP дозволяє створювати шаблони та робочі процеси для відповідності стандартам HIPAA, GDPR та PCI DSS, забезпечуючи дотримання регулятивних вимог.

Symantec DLP використовує шифрування та ідентифікацію доступу для забезпечення безпеки даних на всіх етапах їхнього життєвого циклу. Система також надає можливість повного знищення відкинутих копій і документів, забезпечуючи їхню безпеку навіть у випадку передачі на мобільні пристрої або віддалені місця.

Інтерфейс Symantec DLP наведено на рис. 3.2.

Рис. 3.2. Інтерфейс Symantec DLP

Proofpoint DLP – це сучасне рішення, яке забезпечує високий рівень захисту даних завдяки своїй хмарній архітектурі. Відрізняючись від застарілих підходів DLP, цей продукт орієнтований на людей, легко керується та має масштабовану хмарну архітектуру, що дозволяє спростити програму захисту даних підприємства.

Proofpoint додає телеметрію як загроз, так і поведінки до вмісту, щоб визначити намір і ризик. Об’єднавши їх у сучасну хронологію, ви зможете зрозуміти, чи є користувач, який ініціював попередження DLP , зламаним, зловмисним чи недбалим [13].

Основним характеристиками Proofpoint DLP є:

• Масштабованість та гнучкість. Хмарна архітектура дозволяє масштабувати датчики, зберігання та використання відповідно до потреб вашого підприємства та сценаріїв використання. Це забезпечує гнучкість і ефективність у керуванні даними.

• Відповідність регулятивним вимогам. Proofpoint DLP відповідає вимогам резидентності даних у США та Європі, таким як GDPR, що гарантує дотримання всіх необхідних регулятивних стандартів.

• Конфіденційність за проєктом. Система забезпечує високий рівень конфіденційності завдяки провідним у галузі контролям доступу на основі атрибутів, що дозволяє захищати дані на всіх етапах їхнього життєвого циклу.

Proofpoint DLP має можливість розширення для інтеграції зі ширшою екосистемою безпеки без необхідності додаткових інженерних зусиль, що дозволяє забезпечити комплексний підхід до захисту даних.

Proofpoint DLP не лише спрощує програму захисту даних, але й забезпечує високу ефективність та надійність завдяки своїй сучасній архітектурі.

Інтерфейс Proofpoint DLP наведено на рис. 3.3.

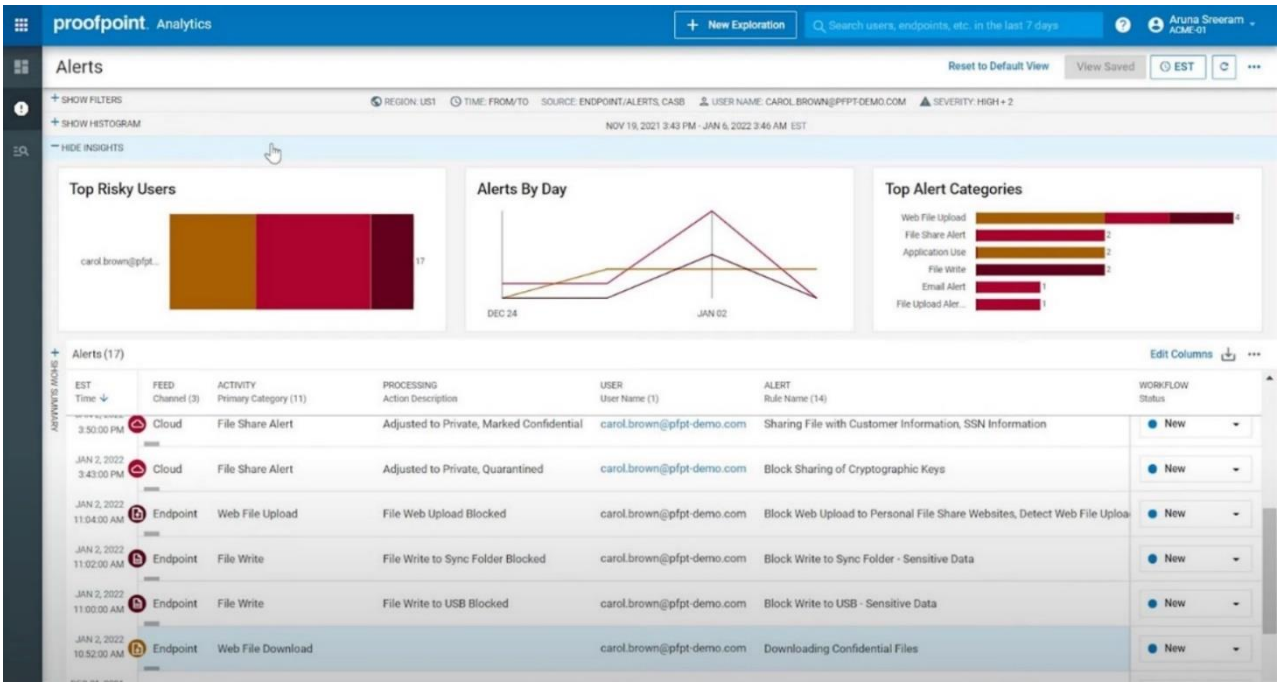


Рис. 3.3. Інтерфейс Proofpoint DLP

Trellix (McAfee) DLP – це комплексне рішення для попередження втрати даних, яке об’єднує захист мережевих, хмарних та кінцевих точок в одному пакеті. Ця система дозволяє ефективно керувати політиками безпеки та

оптимізувати робочі процеси інцидентів завдяки гнучким параметрам розгортання.

Trellix DLP пропонує широкий спектр функцій для забезпечення надійного захисту даних:

• Система має розширені можливості класифікації, що дозволяють ідентифікувати та класифікувати дані за 42 категоріями, забезпечуючи точний контроль над інформацією.

• McAfee DLP може шифрувати, перенаправляти, поміщати на карантин або блокувати передачу даних, що порушують встановлені політики, забезпечуючи надійний захист від втрати даних.

• Система забезпечує централізоване управління всіма інцидентами та звітами, що дозволяє швидко і ефективно реагувати на будь-які загрози.

• Локальні та хмарні політики DLP синхронізуються за допомогою McAfee, забезпечуючи узгодженість та ефективність у захисті даних на всіх рівнях.

Trellix DLP пропонує зручну єдину консоль для керування розгортанням, адміністрування політик, моніторингу подій у режимі реального часу та отримання готових звітів для забезпечення відповідності [14].

Інтерфейс Trellix DLP наведено на рис. 3.4.

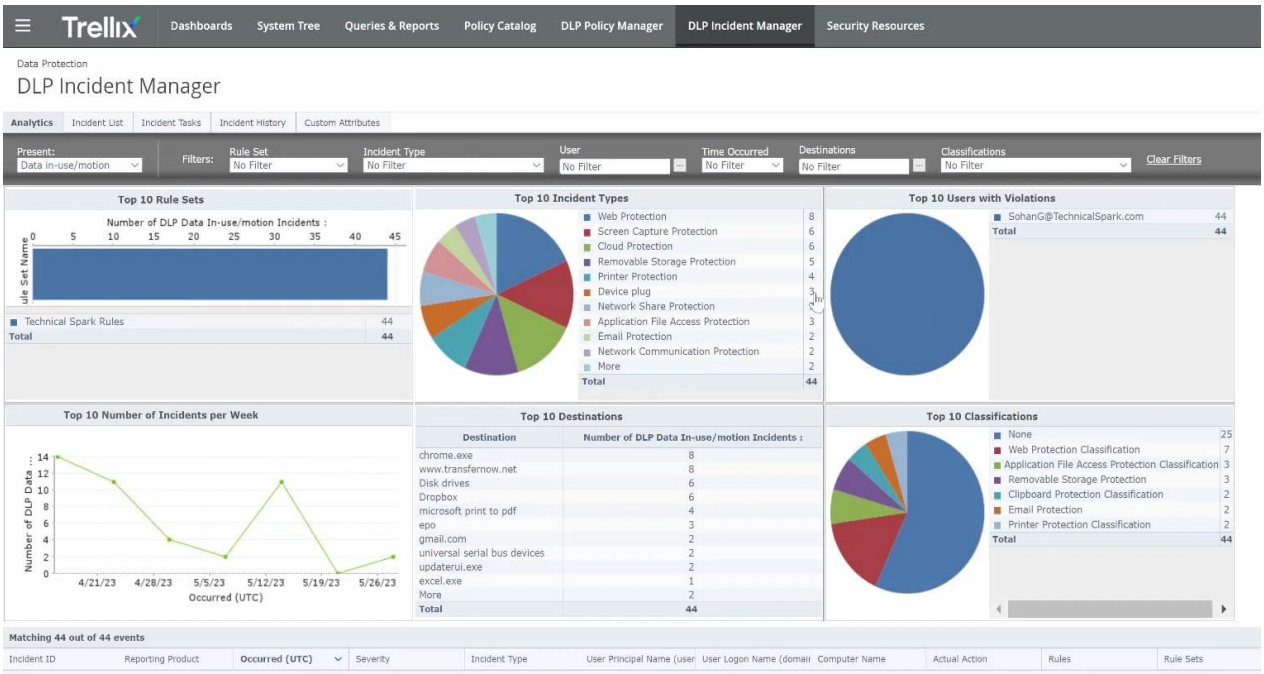


Рис. 3.4. Інтерфейс Trellix DLP

Endpoint Protector від CoSoSys – це потужне рішення для запобігання втрати даних (DLP), яке забезпечує захист інтелектуальної власності (IP), особистої інформації (PII) та від внутрішніх загроз. Це рішення допомагає підприємствам відповідати нормативним вимогам і забезпечувати конфіденційність даних, використовуючи передові технології для виявлення, моніторингу та контролю передачі даних.

Опис основних характеристик Endpoint Protector:

• Endpoint Protector має низку ключових характеристик, що забезпечують надійний захист даних:

• Захист інтелектуальної власності (IP). Використовуючи передові технології, такі як категоризація тексту на основі N-грамів, Endpoint Protector точно виявляє IP, наприклад вихідний код, у сотнях форматів файлів, відстежуючи та контролюючи будь-які передачі даних.

• Захист особистої інформації (PII). За допомогою модуля виявлення даних, Endpoint Protector дозволяє виявляти та захищати особисту інформацію,

що зберігається на комп'ютерах співробітників, запобігаючи її викраденню за допомогою універсального інструменту запобігання втрати даних.

• Захист від внутрішніх загроз. Система зупиняє витік даних, застосовуючи відповідні засоби контролю кібербезпеки на пристроях, від реєстрації потенційних інсайдерських загроз до блокування в режимі реального часу. Вона допомагає виявляти користувачів, які не дотримуються найкращих методів захисту даних, і ситуації, які можуть призвести до порушення політики.

• Відповідність нормативним вимогам. Endpoint Protector допомагає підприємствам забезпечити конфіденційність даних і досягти нормативної відповідності HIPAA, PCI-DSS, GDPR, SOX (Sarbanes-Oxley Act) та іншим стандартам, уникнувши штрафів та інших збитків, накладених регуляторними органами.

Endpoint Protector дозволяє повністю контролювати підключені пристрої та потоки даних на одній інформаційній панелі – навіть віддалено. Отримуйте сповіщення та звіти в режимі реального часу, налаштовуйте політики та використовуйте детальну інформацію та журнали, пов’язані з подіями, передачею файлів, використовуваними пристроями чи діяльністю користувачів, необхідні для швидшого й точнішого зменшення негативних наслідків інцидентів пов'язаних з безпекою даних [15].

Інтерфейс Endpoint Protector від CoSoSys наведено на рис. 3.5.

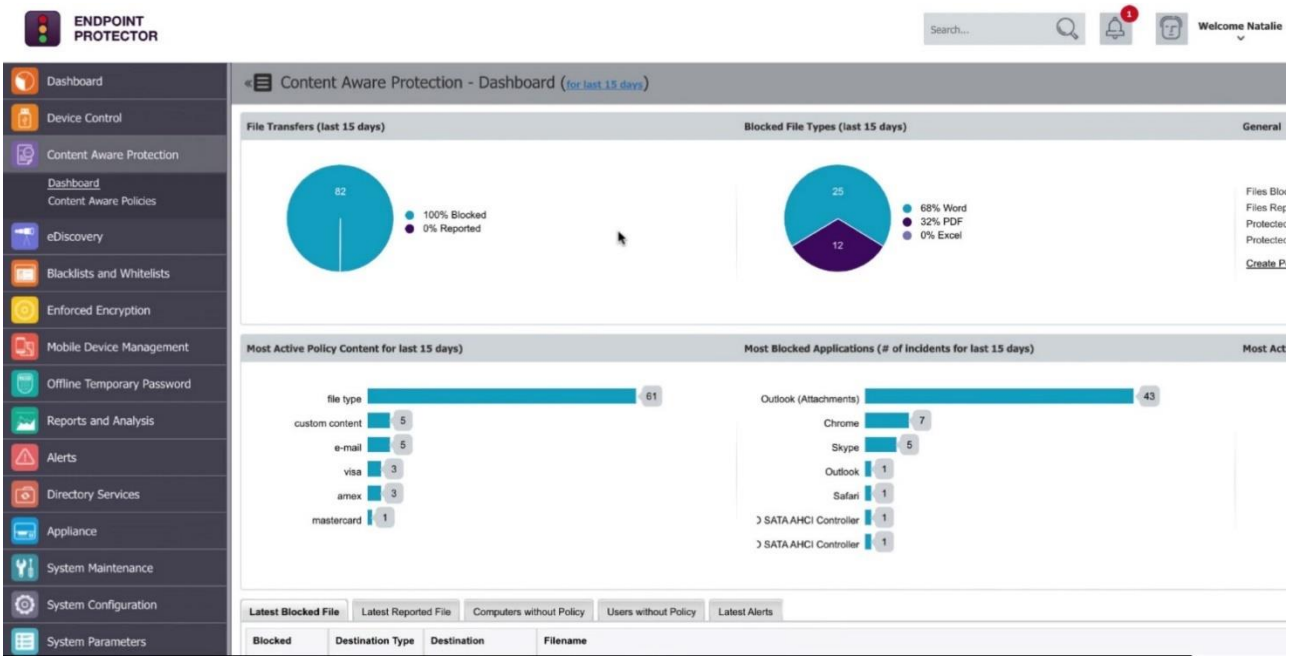


Рис. 3.5. Інтерфейс Endpoint Protector від CoSoSys

З кожним днем DLP-рішення на ринку стають більш модифікованими відповідно до вимог клієнтів. Враховуючи вищезазначену інформацію, не важко зрозуміти, що всі сучасні DLP-системи, які нині є найбільш популярними відповідно до онлайн-платформи Гартнера, подібні одна до одної. Для того, щоб обрати краще DLP-рішення варто проаналізувати основні функціональні можливості кожної з них, за якими орієнтуються пересічні клієнти при виборі.

Порівняння функціональних можливосте DLP-рішень наведено в табл. 3.1.

Таблиця 3.1.

Порівняння функціональних можливосте DLP-рішень

Функціонал / DLP	Підтримка нормативної відповідності	Шифрування	Моніторинг мережі	Безкоштовне випробування
Forcepoint	+	+	+	+
Symantec	+	+	+	-
Proofpoint	+	+	-	+
Trellix (McAfee)	+	+	+	-
Endpoint Protector (CoSoSys)	+	+	+	+

В результаті аналізу основного функціоналу сучасних DLP-рішень провідні позиції заняли такі:

• Forcepoint

• Proofpoint

• Endpoint Protector (CoSoSys)

При виборі того чи іншого DLP-рішення клієнти завжди звертають увагу на такий важливий пункт, де вказано які операційні системи підтримуються. Отже, варто проаналізувати їх за критерієм – підтримка ОС.

Порівння DLP-рішення за підтримкою операційних систем наведено в табл. 3.2.

Таблиця 3.2.

Підтримка операційних систем

DLP / ОС	Force point	Symantec	Proof point	Trellix (McAfee)	Endpoint Protector (CoSoSyS)
Windows	+	+	+	+	+
Mac	+	+	+	+	+
Linux	+	+	-	-	+
Тонкий клієнт	-	-	-	-	+

До ключових критерії при виборі DLP можна віднести методи розгортання, які вони підтримуються. Адаптивність розгортання може суттєво вплинути на те, наскільки легко інтегрується рішення з наявною інфраструктурою. Різні підприємства мають різні потреби та обмеження, і DLP-рішення, яке підтримує кілька методів розгортання, може ефективно задовольнити ці різноманітні вимоги.

Порівння DLP-рішення за методами розгортання наведено в табл. 3.3.

Таблиця 3.3.

Порівння DLP-рішення за методами розгортання

DLP / Розгортання	Force point	Symantec	Proof point	Trellix (McAfee)	Endpoint Protector (CoSoSyS)
On-premise	+	+	-	+	+
Virtual Desktop Infrastructure	-	+	-	-	+
SaaS	+	+	+	-	+

За результатами порівняльного аналізу сучасних популярних DLP-рішень було встановлено, що найбільш якісним є програмний продукт Endpoint Protector від CoSoSys. Окрім того, що цей продукт вміщає в собі основний функціонал, він також підтримує такі ОС, як: Windows, Linux, Mac та ще й може встановлюватися на тонкі клієнти. До тогож, Endpoint Protector адаптований до таких видів розгортань: On-premise, VDI та SaaS. Це означає, що він може задовольнити ключові потреби підприємств, забезпечуючи гнучкість та ефективність в управлінні.

3.2 Застереження при впровадженні DLP-системи

Хоча рішення DLP пропонують надійний захист від витоку даних, їх впровадження вимагає ретельного розгляду та планування. Невиконання цього може призвести до небажаних наслідків і перешкодити досягненню цілей підприємства. Таким чином, важливо підходити до впровадження DLP з обережністю.

На початковому етапі впровадження системи запобігання витоку даних підприємство визначає, навіщо їй DLP-система і який сегмент бізнесу потрібно захистити. Наприклад, підприємство підозрює, що хтось із відділу розробки передає конфіденційні дані третім особам, тоді їй потрібна DLP-система, щоб відстежувати комунікації і переміщення документів в цьому сегменті, а також краще контролювати своїх співробітників.

Однак, обираючи DLP-рішення, кожне підприємство повинне врахувати унікальні характеристики своєї інфраструктури та ступень інформації з обмеженим доступом. Вибір DLP-рішення повинен враховувати ці специфічні потреби, щоб в подальшому можна було забезпечити оптимальний захист. До того ж, читаючи відгуки про привабливе рішення, варто звернути увагу на характеристику «Технічна підтримка та обслуговування», адже це може бути критичним для успішної інтеграції та ефективного використання рішення.

Проте, вищезазначеної інформації не достатньо для того, щоб оцінити обране DLP-рішення, адже все завжди пізнається на практиці. Тому одною із ключових характеристик при виборі рішення є «пробний період використання», адже часто рішення може бути складним у впровадженні та вимагати значних зусиль для налаштування правильних політик безпеки. Недостатня конфігурація може призвести до недооцінення загроз або спровокувати велику кількість помилкових сповіщень, що може перенавантажити адміністраторів.

Також під час пробного періоду необхідно провести ретельну оцінку потенційного впливу DLP-системи на продуктивність мережі та користувачів, оскільки некоректне впровадження може призвести до зниження швидкості роботи мережі, а також негативно позначитися на робочому процесі співробітників.

Коли мета поставлена, сегмент бізнесу визначено та навіть успішно інтегровано DLP-рішення, потрібно більш детально розглянути ситуацію. На цьому етапі будується тактика і стратегія захисту:

1) Підприємство визначає які саме документи або дії співробітників вимагають пильного спостереження і на яких робочих станціях або серверах зберігаються важливі файли. На основі цього створюється політика обробки даних. Ця політика визначає класи даних, які потребують різних типів обробки. Як правило, щонайменше три типи даних класифікуються на основі важливості інформації та шкоди, яку може спричинити її неправильне використання або втрата:

- Дані високого рівня ризику включають конфіденційні дані та інтелектуальну власність, які можуть завдати великої шкоди в разі втрати або зламу.

Якщо підприємство працює в регульованій галузі, політика обробки даних має вирішувати такі питання, як дотримання стандартів безпеки, конфіденційності та нормативних актів, таких як HIPAA та GDPR. Інформація, що підпадає під нормативні стандарти, майже завжди потрапляє до категорії високого рівня ризику;

- Дані середнього рівня ризику можуть завдати підприємству меншої шкоди. Вони можуть містити щось, чим зацікавляться конкуренти, але це не спричинить негативного впливу на бізнес;
- Дані з низьким рівнем ризику не потребують додаткового захисту та можуть вільно поширюватися серед громадськості. Інформативні посібники та інструкції користувача, які допомагають клієнтам використовувати продукти компанії, є прикладами даних із низьким ризиком.

Політика обробки даних є основою, на якій будується стратегія DLP, тому варто приділити час, щоб її правильно розробити.

2) Відповідно до політики обробки даних адміністрації обов'язково потрібно створити користувацькі ролі та розподілити співробітників за ними, що забезпечити доступність до інформації відповідно до наданих повноважень.

3) Після визначення політики обробки даних, підприємство має забезпечити конфіденційність інформаційних ресурсів. Це передбачає виявлення даних у всьому інформаційному середовищі для подальшої їх класифікації.

4) Після класифікації даних підприємство формує політики безпеки, які складаються з різних правил, за допомогою яких DLP-система зможе ідентифікувати дії або ситуації деструктивного характеру, які несуть за собою пряму або потенційну загрозу. Прикладами таких дій є:

- Обмін конфіденційними даними електронною поштою;
- Передача даних високого ризику з віддалених кінцевих точок;
- Зберігання конфіденційних даних у публічному хмарному сховищі;
- Тощо.

Якщо хтось із співробітників порушить встановлені правила, система сповістить аналітика з ІБ про інцидент, який буде діяти відповідно до зазначених інструкцій.

Запровадивши підходяще DLP-рішення, потрібно забезпечити якісне відстеження руху даних. Постійний нагляд за переміщенням даних є ключовим для успішної стратегії DLP. Кожен випадок передачі чи доступу до даних повинен відповідати встановленій політиці обробки даних. Це охоплює всі внутрішні та зовнішні дії щодо ресурсів даних.

В подальшому, адміністрації підприємства потрібно створити для співробітників інструкції поводження з корпоративними даними, щоб зменшити ризик виникнення незрозумілих ситуацій.

3.3 Пропозиції щодо підвищення ефективності DLP-систем

Ефективність системи запобігання втраті даних нерозривно пов’язана з інтенсивністю праці, вкладеної в її налаштування та обслуговування. Побудова ефективної DLP-системи вимагає багатоетапного процесу: визначення даних, які потребують захисту, розуміння ризиків для боротьби, налаштування політик і технологій аналізу, моніторингу й аналіз подій, а також постійної адаптація політик на основі виникнення нових ідей або загроз (рис. 3.6.).

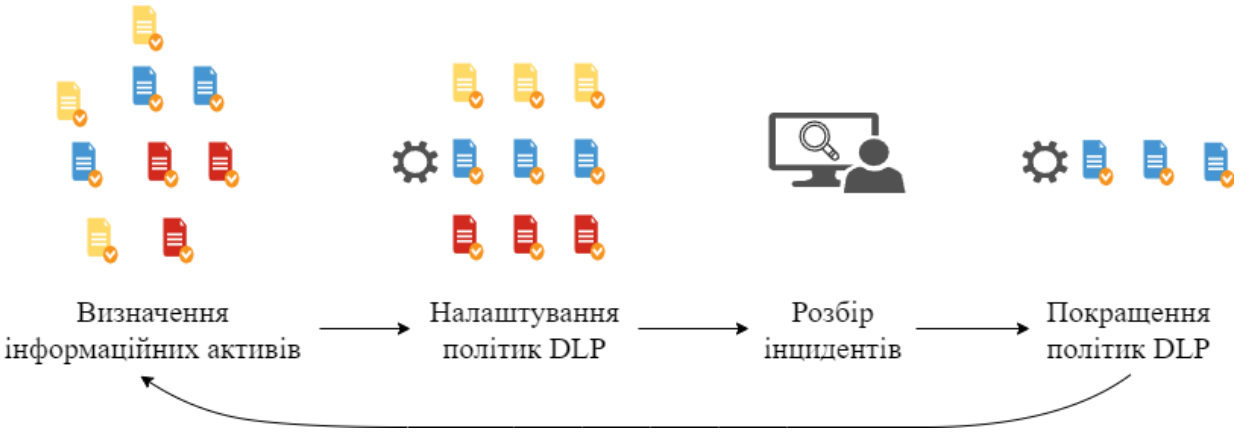


Рис. 3.6. Процес побудови DLP-системи

Зрозуміло, що для запобігання витоку тієї чи іншої конфіденційної інформації, підприємство повинне визначити які дані можна віднести до цеї

групи та класифікувати їх за ступенем необхідної захищеності. І для того, щоб реалізувати це, необхідно розуміти, що даний процес повинен складатися не лише з ідентифікації очевидних зразків критично важливих документів, але й з розпізнавання будь-яких згадувань та посилань на ці документи в різних каналах зв'язку таких, як електронна пошта та месенджери. Для цього потрібно створити складну лінгвістичну модель, яка не складається тільки з декількох десятків яких-небуть виразів, а повинна в собі містити сотні термінів, враховуючи їхні зв'язки та пріорітетність кожного з них.

Розробка такої лінгвістичної моделі трудомістка і забирає багато часу. Як правило, створення надійного лінгвістичного словника займає близько 10 днів. Для цього треба взяти зразки документів, проаналізувати їх і виділити які терміни відносяться до ключових, а які ні. Для побудови повноцінної лінгвістичної моделі потрібен кваліфікований лінгвіст. На основі такої модель і будуються різноманітні політики.

Проблема полягає в тому, що заснування політики також потребує кропіткої роботи та є фінансовозатратним заняттям, адже спочатку вона створюєть, потім її треба протестувати, поборотися з хибнонегативними та хибнопозитивними спрацьовуваннями системи.

Отже, впровадження ефективної політики займає приблизно 1–2 місяці, і це призводить до того, що переважна більшість підприємств ретельно оновлює політики тільки раз в рік. Тому сприючись не все вищезазначе, однією із пропозицій є підвищення ефективності використання DLP, шляхом перекладення деяких задач на штучний інтелект.

Серед сучасних DLP-рішень, які займають верхні позиції на ринку, деякі з них пропонують використовувати технологію, яка назвиється автолінгвіст. Скористатися цією технологією дуже просто. Для цього необхідно всього лише зібрати всю необхідну документації буль-якого формату (pdf, rtf, doc, docx, xls та інші), після цього направити їх на обробку до автолінгвіста. В результаті через декілька хвилин він сформує новий лінгвістичний словник з десятками тисяч термінів (рис. 3.7.).

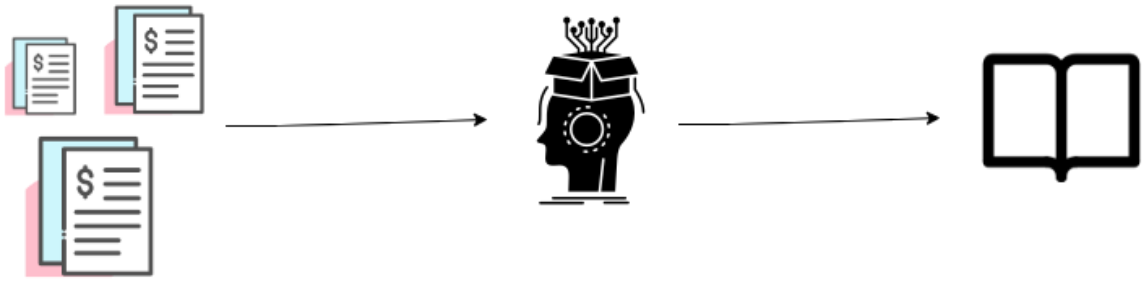


Рис. 3.7. Процес роботи автолінгвіста

Після цього підприємство може актуалізувати свої політики в будь-який момент при потребі. Однак, щоб досягнути цього, треба навчати автолінгвіста.

ШІ використовується в різних галузях, але на ринку DLP-рішень залишається помітний скептицизм. Багато представників клієнтів висловлюють свою недовіру до технологій ШІ з кількох причин. Дехто сприймає штучний інтелект лише як тренд, хвилю ажіотажу, яка з часом спаде. Інші вважають, що штучний інтелект все ще є незрілою, недостатньо розвиненою технологією, яка не готова для таких важких завдань, як захист даних. Крім того, дехто впевнений, що традиційних методів, не пов’язаних зі штучним інтелектом, достатньо для їхніх потреб при використанні DLP. Незважаючи на ці застережння, ШІ має значні переваги. Через те, що детерміновані підходи і статичний аналіз вже являються не актуальни, різні вендори додають до своїх DLP-рішень можливість використовувати ШІ.

Налаштування політик в будь-якій DLP-системі не може бути ідеальним. Завжди рано чи пізно випливає трафік, який не належить до жодної зі створених категорії для подальшої класифікації. Такий трафік як правило потрапляє в «сіру зону». Проаналізувати вручну весь такий трафік неможливо, але за рахунок ШІ цю проблему можна швидко вирішити. Технологія, яка знаходить нові категорії документів, групує їх і рекомендує захистити, називається Data Explorer (рис. 3.8.).

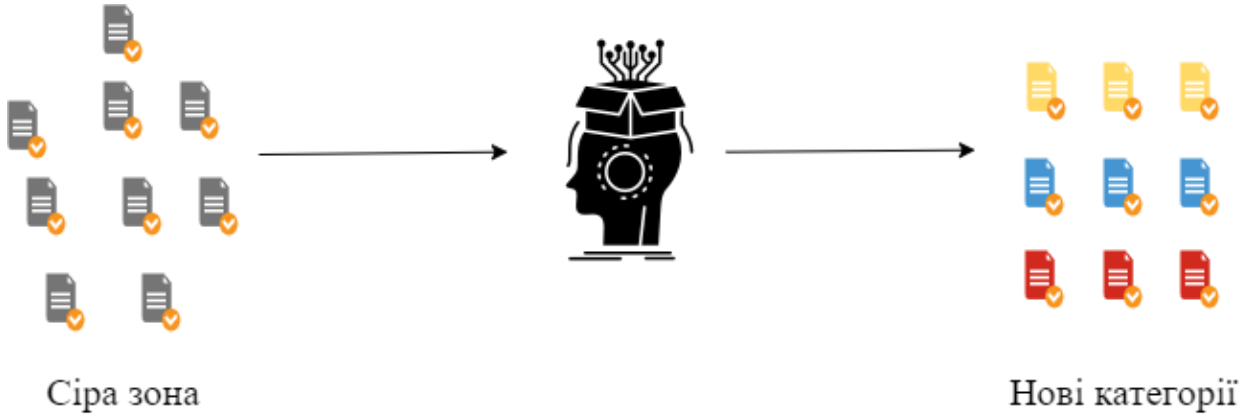


Рис. 3.8. Процес роботи Data Explorer

Data Explorer не потребує подальношого навчання. Ця технологія автоматично катигорізує весь трафік. Така система породжує процес періодичної протидії хибнонегативним спрацьовуванням.

Варто зазначити, що деякі нові технології на основі ШІ в DLP-системах створені для того, щоб виявлети графічну конфіденційну інформації, а також дають можливість передбачити ризики та загрози, пов'язані зі співробітниками, виявляти аномальну поведінку працівників на робочому місці.

Наступні пропозиції для підвищення ефективності пов’язані з інтеграцією DLP системи із іншими технологіями.

Одним із найбільш перспективних варіантів розширення функціоналу DLP систем є інтеграція з SIEM технологією. У симбіозі системи взаємно доповнюють одна одну. Компоненти DLP-системи здійснюють пошук і класифікацію інформації, що захищається за встановленими критеріями. А SIEM формує «єдине вікно» для адміністратора безпеки, в якому зводяться дані про виявлені файли, що підлягають захисту, спроби доступу до них, а також корелюється технологічна інформація, що надходить від ОС, системи управління базами даних (СУБД), мережевого обладнання та інших джерел, формуючи повну картину стану інформаційної безпеки на підприємстві [16].

Якщо підприємство не в змозі фінансово підтримувати DLP-систему з додатковими технологіями на основі ШІ або ж занадто дорогою виявляється інтеграція з SIEM, то більш економнішим рішенням є можливість ітегрування DLP разом з DCAP-системою.

Системи DCAP класифікує усі документи в компанії на основі їх змісту. Вони сканують сховища та читають файли, а потім класифікують їх у різні групи, наприклад особисті дані, фінансові звіти, контракти тощо. Кожній категорії присвоюється певна мітка, яка застосовується до файлу у файловій системі. Ця мітка діє як «обкладинка» для файлу, вказуючи системам захисту від втрати даних (DLP), що файл містить конфіденційний або вразливий вміст. DCAP розширює можливості керування інцидентами за межі того, що можуть відстежувати системи DLP. Наприклад, коли у працівника знайшовся документ, який не призначений для нього, а система DLP через якусь причину не виявила передачі файлу, тоді DCAP може надати важливу інформацію про те, як цей документ потрапив до нього: покаже, що файл спочатку зберігався в спільній папці та що співробітник скопіював його на свій персональний комп’ютер. Цей рівень деталізації необхідний для розуміння контексту потенційних порушень безпеки та запобігання подібним інцидентам у майбутньому.

Інтегруючи DCAP із DLP, підприємства можуть створити більш комплексну систему безпеки. DCAP не тільки класифікує та позначає конфіденційну інформацію, але й відстежує шаблони доступу до файлів і переміщення документів в межах підприємства.

Висновки до розділу 3

На основі проведеного порівняльного аналізу сучасних популярних DLP-рішень було встановлено, що найбільш якісним є програмний продукт Endpoint Protector від CoSoSys. Цей продукт може задовольнити ключові потреби підприємств, забезпечуючи гнучкість та ефективність в управлінні.

Впровадження DLP-систем не обходиться без певних викликів і застережень. Важливо ретельно планувати процес інтеграції, враховуючи специфіку роботи підприємства та потенційні ризики.

Для підвищення ефективності DLP-систем було розроблено кілька рекомендацій. По-перше, слід розглянути можливість делегування частини завдань на штучний інтелект. Використання алгоритмів машинного навчання та інших ШІ-технологій може значно покращити здатність системи до виявлення та реагування на загрози в режимі реального часу. Це дозволяє зменшити кількість помилкових спрацьовувань та підвищити точність аналізу даних.

По-друге, рекомендується інтегрувати DLP-систему з SIEM або DCAP. Така інтеграція дозволяє забезпечити більш комплексний підхід до безпеки даних, об'єднуючи можливості моніторингу, аналізу та реагування на інциденти.

Дотримання зазначених рекомендацій та застережень при впровадженні DLP-системи сприятиме підвищенню рівня інформаційної безпеки на підприємстві та забезпеченню надійного захисту конфіденційних даних.

ВИСНОВКИ

У дослідженні було детально розглянуто системи запобігання витоку інформації (DLP) з метою забезпечення інформаційної безпеки на підприємствах. Основним об’єктом аналізу стали різні види DLP-систем та принципи їх функціонування, а предметом – особливості цих рішень для подальшого впровадження в корпоративних середовищах.

Для вирішення поставленого наукового завдання застосовувалися методи аналізу, порівняння, класифікації, експертної оцінки та системного підходу. У результаті дослідження доведено критичну важливість захисту інформаційної безпеки для підприємств. Зокрема, було проведено порівняльний аналіз сучасних популярних DLP-рішень і виявлено, що найякіснішим продуктом є Endpoint Protector від CoSoSys, який відзначається високою надійністю та ефективністю.

Крім того, під час дослідження було виявлено ключові аспекти функціонування DLP-систем і сформовано застереження для їх впровадження, що дозволяють уникнути потенційних проблем і ризиків. Для підвищення ефективності DLP-систем були розроблені рекомендації, серед яких особливо важливими є делегування частини завдань штучному інтелекту та інтеграція DLP-систем з SIEM або DCAP. Це дозволяє створити комплексний підхід до безпеки даних, об’єднуючи можливості моніторингу, аналізу та реагування на інциденти.

Результати цього дослідження мають практичне значення і можуть бути застосовані при плануванні та реалізації систем управління інформаційною безпекою на підприємствах. Впровадження розроблених рекомендацій сприятиме підвищенню ефективності існуючих DLP-рішень, забезпечуючи надійний захист конфіденційної інформації від несанкціонованого доступу та витоку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 16.12.2020 р. № 1089-IX. URL:
https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

2. Share of organizations worldwide that have experienced a loss of sensitive information as of February 2023, by country. URL:
https://www.statista.com/statistics/1387392/loss-sensitive-information-organizations-worldwide-by-country/

3. Про інформацію: Закон України від 1992 р № 48. URL:
https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. Бурцева К. А., Тимофєєв Д. С. Підвищення рівня інформаційної безпеки за допомогою підприємствних заходів на комерційних підприємствах. URL:
https://ir.nmu.org.ua/bitstream/handle/123456789/1673/6.pdf?sequence=1

5. Бондаренко О. Джерела виникнення каналів витоку інформації. URL:
https://prezi.com/p/qdc4r9aihlum/presentation/

6. Тлумак О. Інформаційна безпека підприємства: сучасні виклики та загрози. URL:
https://ena.lpnu.ua:8443/server/api/core/bitstreams/7cbea921-7393-42a4-91d4-364acc52e304/content

7. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. Київ : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 189 с.

8. Розділ 13. Відновлення функціонування інформаційно-комунікаційних систем (ІКС) після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. URL:
https://e-tk.lntu.edu.ua/pluginfile.php/25324/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2013.pdf

9. Що таке багатофакторна автентифікація та коли доцільно її використовувати. URL:

https://yubikey.com.ua/shcho-take-bahatofaktorna-avtentyfikatsiia-ta-koly-dotsilno-ii-vykorystovuvaty

10. Вовчановський П. П., Демчинський В. В. Архітектура dlp-систем в умовах політики byod. URL:

https://ela.kpi.ua/server/api/core/bitstreams/adc8cab3-46e8-40fe-9181-ed4f2428fa4f/content

11. Forcepint. Prevent Data Breaches with Data Loss Prevention. URL:

https://www.forcepoint.com/data-loss-prevention

12. The Best Data Loss Prevention Software Tools. URL:

https://www.comparitech.com/data-privacy-management/data-loss-prevention-tools-software/

13. Proofpoint. Enterprise Data Loss Prevention. URL:

https://www.proofpoint.com/au/products/information-protection/enterprise-dlp

14. Trellix Data Loss Prevention. URL:

https://www.trellix.com/products/dlp/

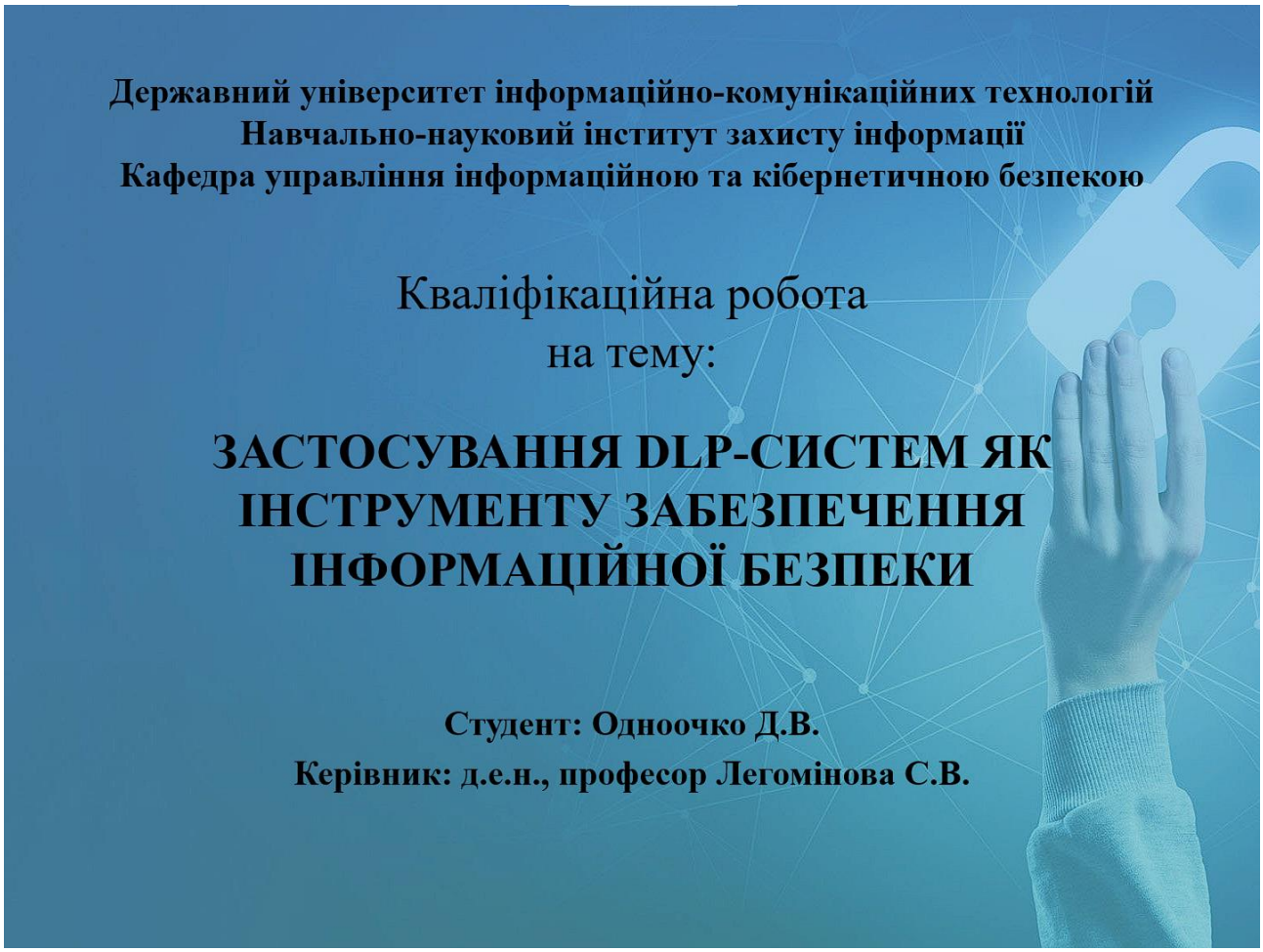
15. Endpoint protector by CoSoSys. Провідне кросплатформне DLP-рішення. URL:

https://www.endpointprotector.com/ua

16. Андриянова Т. А., Саломатин С.Б. Симбиоз SIEM и DLP. URL:

https://libeldoc.bsuir.by/bitstream/123456789/26966/1/Andriyanova_Simbioz.PDF

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)



АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

На сьогодні захист інформації від витоку є одною із найбільш актуальних тем. В епоху, коли обмін інформацією стає все більш інтенсивним та необхідним для бізнесу, захист конфіденційних даних стає завданням першочергового значення, адже організації почали частіше стикатися з різноманітними загрозами, такими як кібератаки, незаконні витоки інформації та порушення конфіденційності.

Порушення безпеки даних може призвести до значних фінансових збитків, пошкодження репутації, юридичних наслідків та втрати довіри з боку клієнтів. У таких умовах DLP-системи стають ключовим інструментом для забезпечення інформаційної безпеки в організаціях різних масштабів.

МЕТА ДОСЛІДЖЕННЯ

Дослідженні DLP-систем для забезпечення інформаційної безпеки на підприємствах.

ЗАВДАННЯ ДОСЛІДЖЕННЯ

1. Дослідити загальні принципи забезпечення інформаційної безпеки, шляхом аналізування статистики витоку даних та існуючих каналів витоку.

2. Проаналізувати DLP-системи та дослідити принципи функціонування їх.

3. Порівняти сучасні рішення DLP, визначити застереження при впровадженні системи запобігання витоку даних та надати пропозиції щодо підвищення ефективності роботи цієї системи.

ОБ’ЄКТ ДОСЛІДЖЕННЯ

DLP-системи різного виду й принципи їх функціонування.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

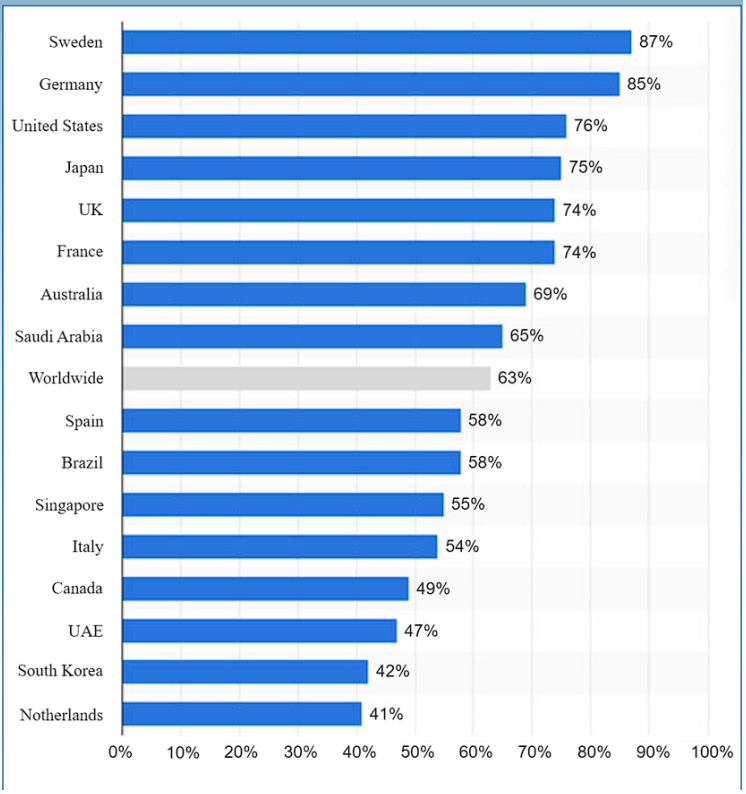
Особливості DLP рішення для подальшого впровадження на підприємствах.

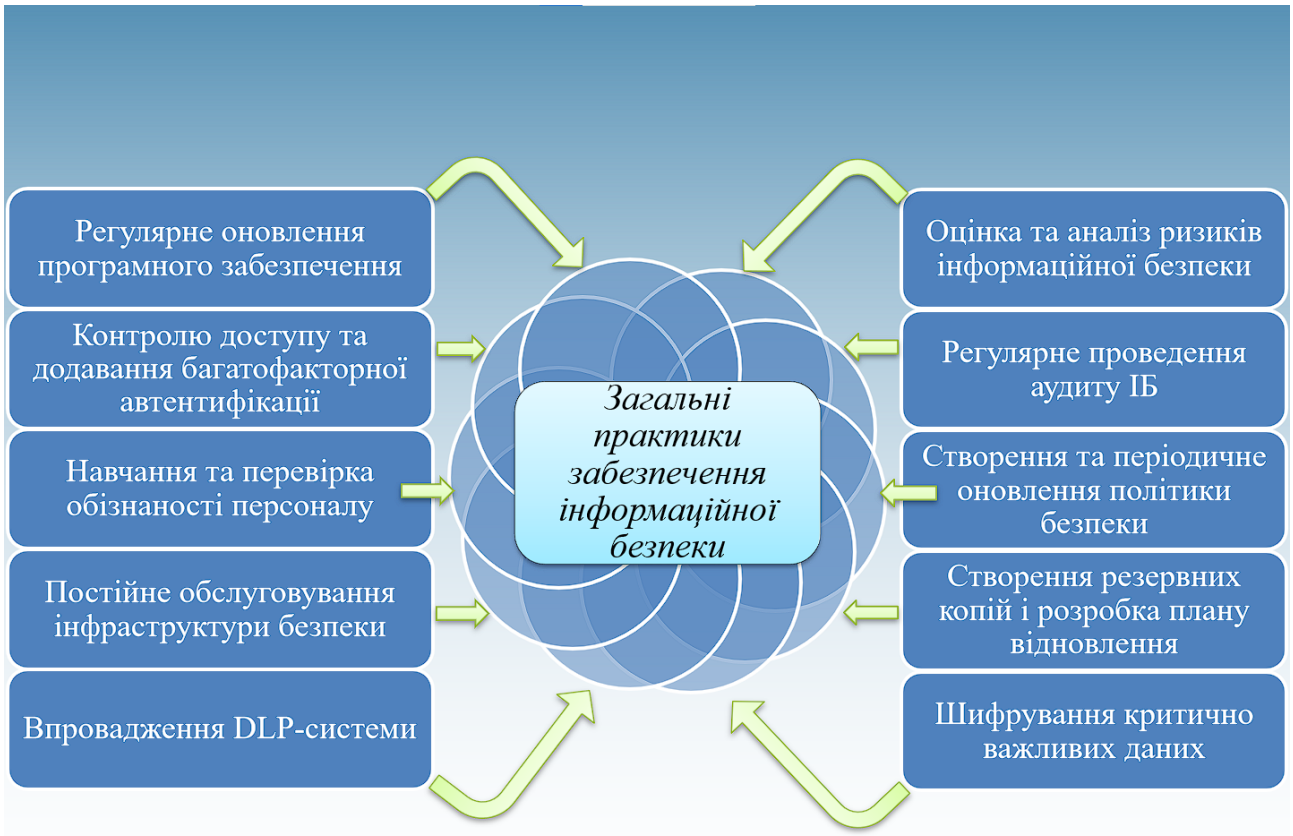
Розділ 1 ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Виток навіть невеликої частини конфіденційної інформації може призвести до серйозних фінансових втрат та порушення репутації компанії.

Групи факторів витоку:

- застосування складних систем обробки інформації;
- збої при роботі серверів;
- виникнення помилок в роботі ПЗ;
- робочий персонал;
- кооперативні об’єднання;
- переїзди до інших офісних приміщень.

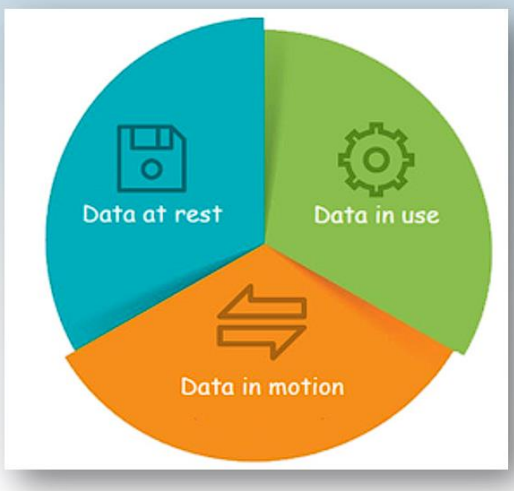



Регулярне оновлення програмного забезпечення
Контролю доступу та додавання багатофакторної автентифікації
Навчання та перевірка обізнаності персоналу
Постійне обслуговування інфраструктури безпеки
Впровадження DLP-системи
Загальні практики забезпечення інформаційної безпеки
Оцінка та аналіз ризиків інформаційної безпеки
Регулярне проведення аудиту ІБ
Створення та періодичне оновлення політики безпеки
Створення резервних копій і розробка плану відновлення
Шифрування критично важливих даних

⑥

Розділ 2 АНАЛІЗ ВИКОРИСТАННЯ DLP-СИСТЕМ

DLP-система (Data Loss / Leak Prevention) – це комплексний набір інструментів та процесів, призначених для виявлення та запобігання незаконному використанню, втраті або витоку конфіденційної інформації в організації.



Функції:

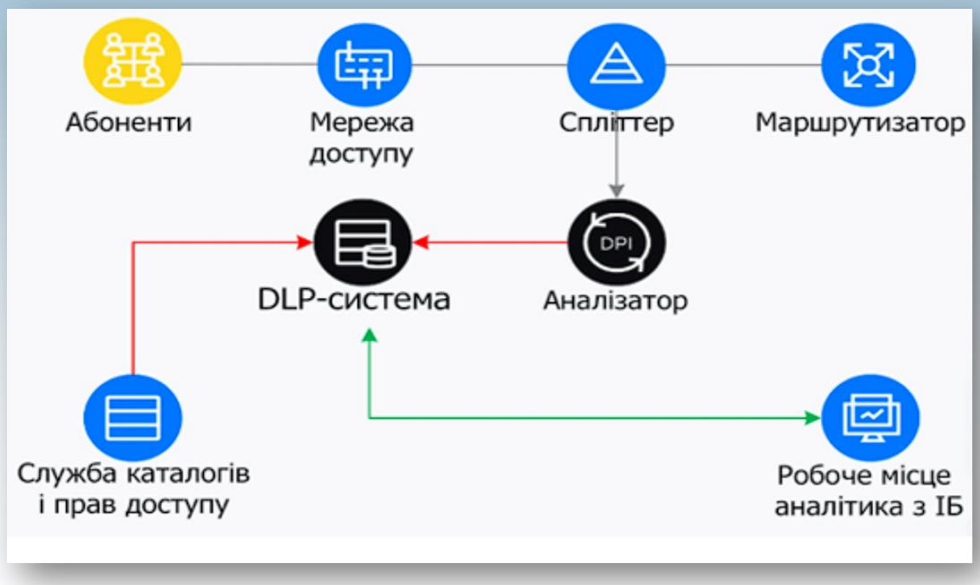
- виявлення та класифікація даних;
- моніторинг;
- блокування передачі даних

у разі необхідності.

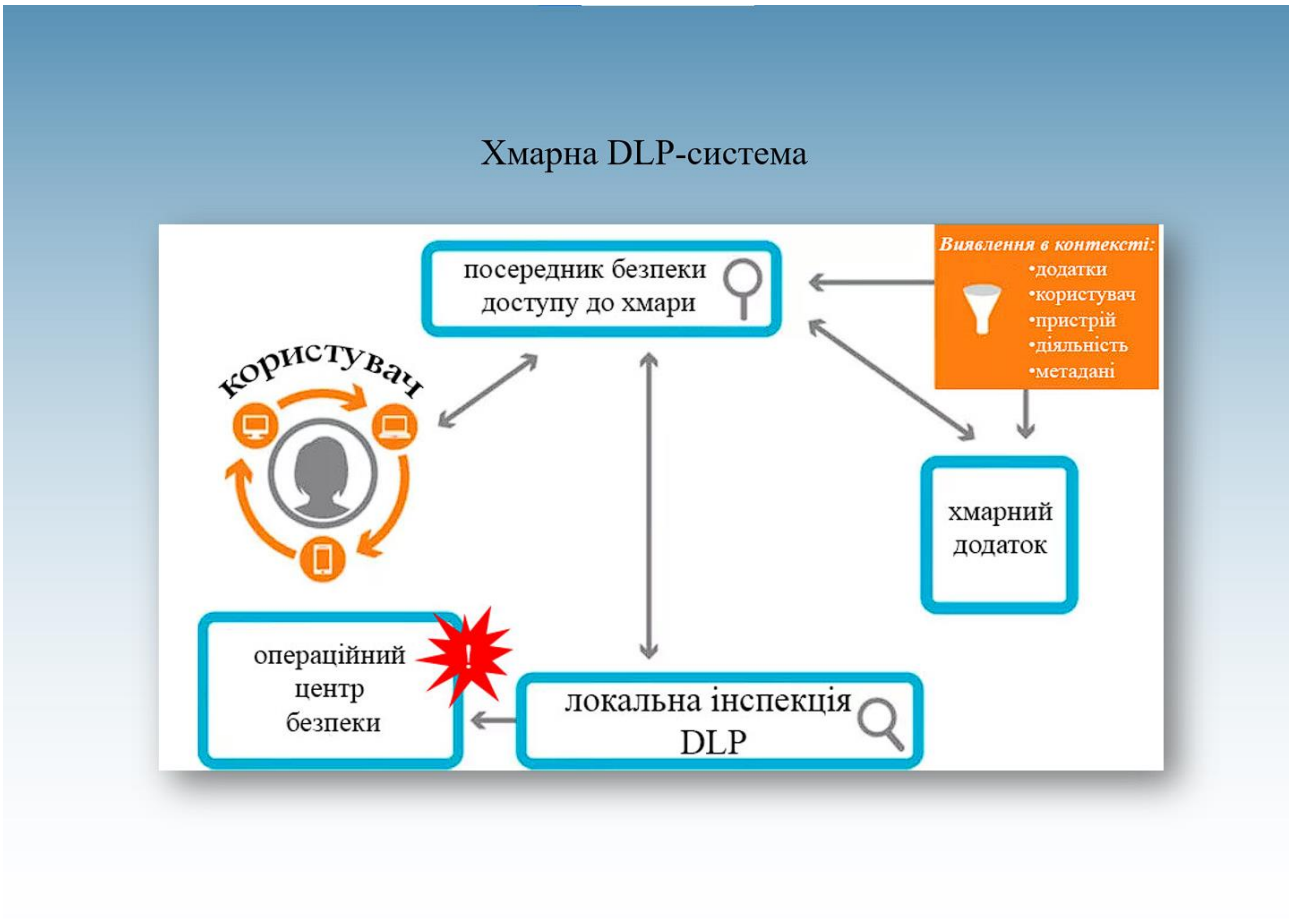
⑦

Види DLP-систем

Мережева DLP-система

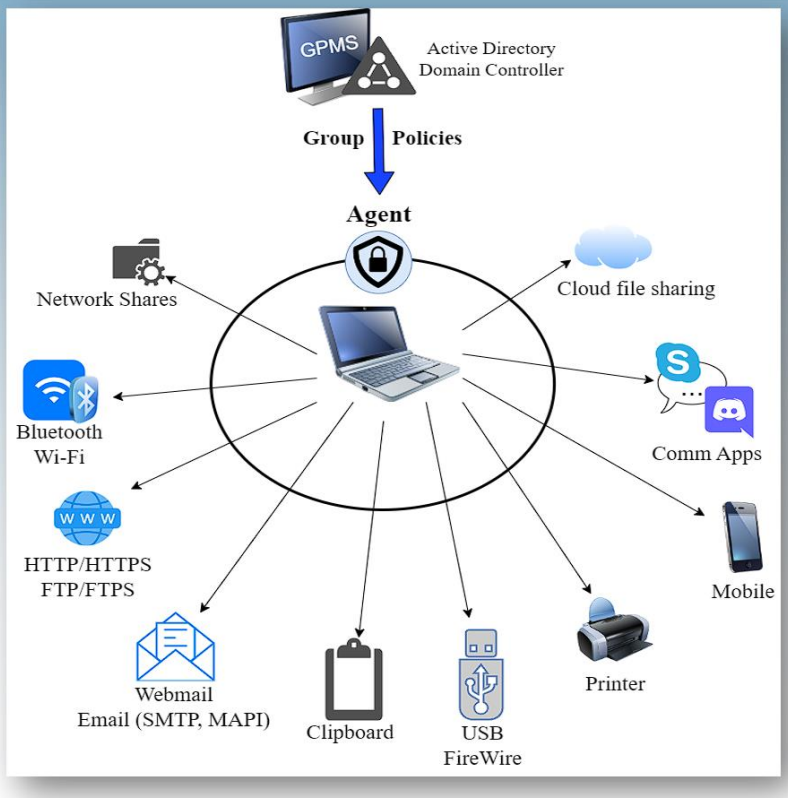


⑧


Хмарна DLP-система
посередник безпеки доступу до хмари
Виявлення в контексті:
•додатки
•користувач
•пристрій
•діяльність
•метадані
користувач
хмарний додаток
операційний центр безпеки
!
локальна інспекція DLP

⑨

DLP-система кінцевих точок



⑩


Методи виявлення конфіденційної інформації
лінгвістичний метод
морфологічний аналіз і стемінг
сигнатурний метод
пошуку в потоці даних певної послідовності символів
мітки
вбудовування спеціальних ідентифікаторів всередині файлів
ручне детектування
ручний аналіз та перевірку конфіденційних даних або файлів
регулярні вирази
використанні спеціальних виразів, які визначають певні правила пошуку тексту
цифрові відбитки
різні типи хеш-функцій для визначення унікальних характеристик

⑪

Розділ 3 ОЦІНКА ТА УДОСКОНАЛЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІ

Порівняльний аналіз сучасних DLP-рішень

- Forcepoint
- Symantec
- Proofpoint
- Trellix (McAfee)
- Endpoint Protector (CoSoSys)

⑫

Порівняння функціональних можливосте DLP-рішень

Функціонал / DLP	Підтримка нормативної відповідності	Шифрування	Моніторинг мережі	Безкоштовне випробування
Forcepoint	+	+	+	+
Symantec	+	+	+	-
Proofpoint	+	+	-	+
Trellix (McAfee)	+	+	+	-
Endpoint Protector (CoSoSys)	+	+	+	+

Підтримка операційних систем

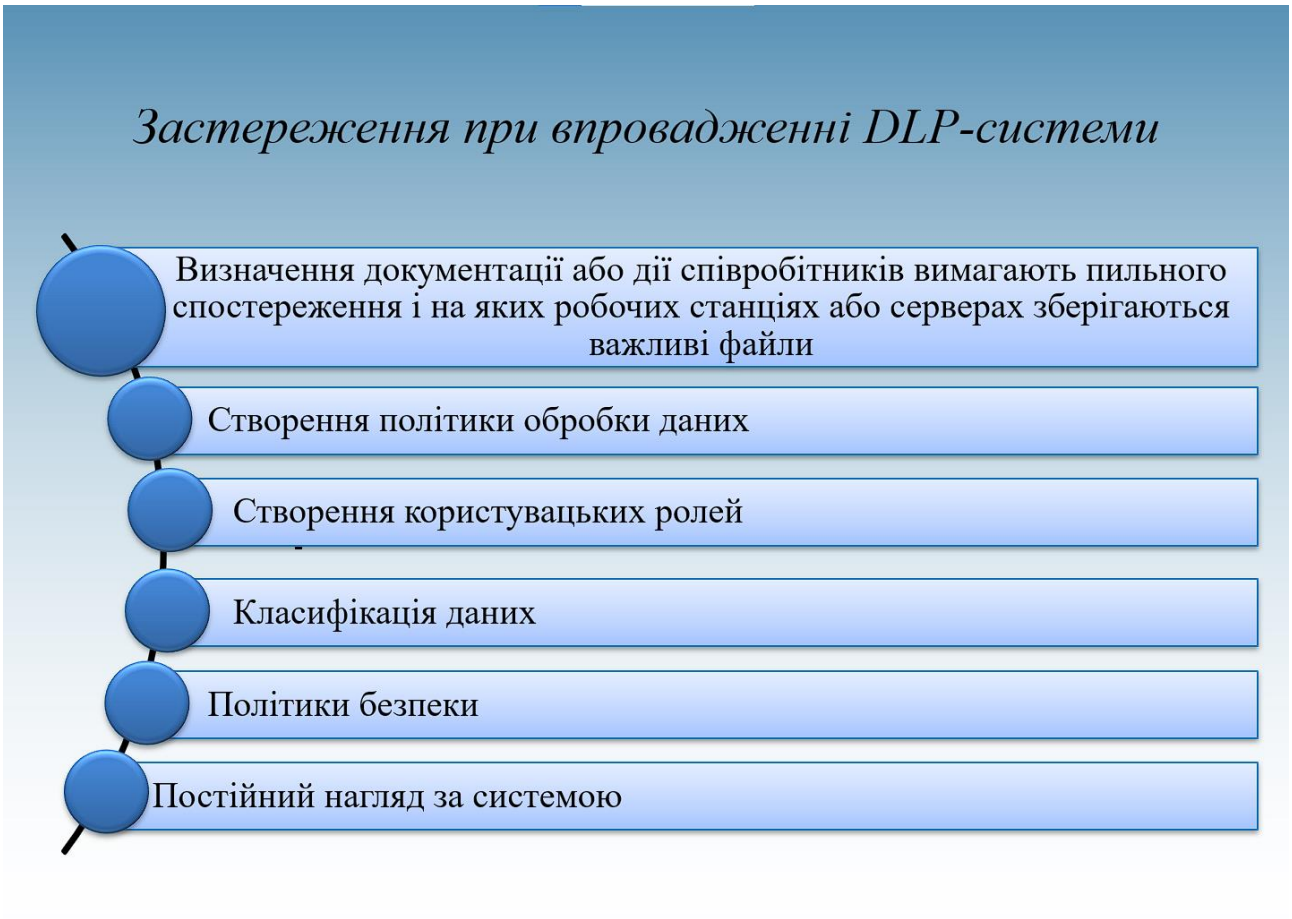
DLP / ОС	Forcepoint	Symantec	Proofpoint	Trellix (McAfee)	Endpoint Protector (CoSoSyS)
Windows	+	+	+	+	+
Mac	+	+	+	+	+
Linux	+	+	-	-	+
Тонкий клієнт	-	-	-	-	+

⑬

Порівння DLP-рішення за методами розгортання

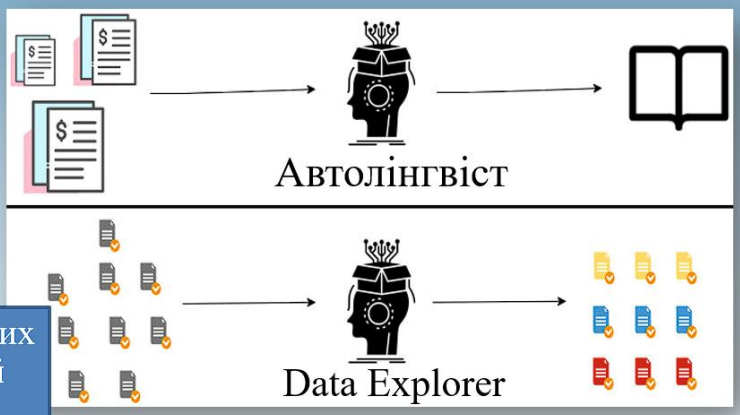
DLP / Розгортання	Forcepoint	Symantec	Proofpoint	Trellix (McAfee)	Endpoint Protector (CoSoSyS)
On-premise	+	+	-	+	+
Virtual Desktop Infrastructure	-	+	-	-	+
SaaS	+	+	+	-	+

За результатами порівняльного аналізу сучасних популярних DLP-рішень було встановлено, що найбільш якісним є програмний продукт Endpoint Protector від CoSoSys. Окрім того, що цей продукт вміщає в собі основний функціонал, він також підтримує такі ОС, як: Windows, Linux, Mac та ще й може встановлюватися на тонкі клієнти. До тогож, Endpoint Protector адаптований до таких видів розгортань: On-premise, VDI та SaaS. Це означає, що він може задовольнити ключові потреби підприємств, забезпечуючи гнучкість та ефективність в управлінні.


Застереження при впровадженні DLP-системи
Визначення документації або дії співробітників вимагають пильного спостереження і на яких робочих станціях або серверах зберігаються важливі файли
Створення політики обробки даних
Створення користувацьких ролей
Класифікація даних
Політики безпеки
Постійний нагляд за системою

⑮

Пропозиції щодо підвищення ефективності DLP-систем



Перекладення деяких задач на штучний інтелект

Інтеграція DLP з SIEM технологією

Інтеграція DLP з DCAP технологією

⑯

ВИСНОВКИ

У кваліфікаційній роботі:

- досліджено загальні принципи забезпечення інформаційної безпеки шляхом аналізування статистики витоку даних та існуючих каналів витоку. Розглянуто основні аспекти, що впливають на інформаційну безпеку організацій, та проаналізовано фактори, що сприяють витоку даних;

- проаналізовано DLP-системи та досліджено принципи їх функціонування. Розглянуто різні методи виявлення конфіденційної інформації;

- проведено порівняння сучасних рішень DLP, визначено застереження при впровадженні системи запобігання витоку даних та надано пропозиції щодо підвищення ефективності роботи цієї системи. Рекомендовано заходи для оптимізації процесу впровадження DLP-систем, а також стратегії для покращення їх продуктивності та надійності в умовах сучасних загроз інформаційній безпеці.

Результати цього дослідження мають практичне значення і можуть бути застосовані при плануванні та реалізації систем управління інформаційною безпекою на підприємствах. Впровадження розроблених рекомендацій сприятиме підвищенню ефективності існуючих DLP-рішень, забезпечуючи надійний захист конфіденційної інформації від несанкціонованого доступу та витоку.

ДЯКУЮ ЗА УВАГУ!