

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту вів витоку даних в організації на основі DLP»

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

_____ Михайло БЕЗПРОЗВАННИЙ

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61

БЕЗПРОЗВАННИЙ Михайло

(прізвище, ім'я)

Керівник

Доктор філософії Педченко Є.М.

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

_____ (науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

Систем та технологій
кібербезпеки

Галина ГАЙДУР
“___” жовтня 2025 року

З А В Д А Н Н Я НА КВАЛІФІКАЦІЙНУ РОБОТУ

БЕЗПРОЗВАННОМУ Михайлу Ігоровичу

(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захисту вів витоку
даних в організації на основі DLP»

керівник кваліфікаційної роботи

Педченко Євген Миколайович, Доктор
філософії

(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних
технологій від «___» жовтня 2025 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи

інформаційні ресурси організації;

рішення ManageEngine;

наукова та технічна література, експлуатаційна документація, нормативні
документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно
розробити)

1. Дослідження проблеми захисту даних в організації та загроз витоку
інформації.

2. Аналіз методів та засобів захисту від витоку даних на основі сучасних DLP-
систем. (ManageEngine)

3. Технологія захисту даних в організації на базі DLP-системи.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту даних та загрози витоку інформації в організації.	01.10.2025 р.	
2.	Аналіз наукової, технічної та нормативної літератури з питань DLP та захисту даних.	12.10.2025 р.	
3.	Аналіз методів та засобів захисту від витоку даних на основі сучасних DLP-систем.	27.10.2024 р.	
4.	Розроблення технології захисту даних в організації на базі DLP-системи. (ManageEngine)	03.11.2025 р.	
5.	Формування рекомендацій щодо впровадження та використання технології DLP у організації.	13.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	25.12.2025 р.	

Здобувач вищої освіти

(підпис)

Михайло
БЕЗПРОЗВАННИЙ
(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Євген ПЕДЧЕНКО
(ім'я, прізвище)

ВІДГУК РЕЦЕНЗЕНТА на кваліфікаційну роботу

здобувача БЕЗПРОЗВАННОГО Михайла

на тему: ««Технологія захисту від витоку даних в організації на основі DLP»

Актуальність: У сучасних умовах стрімкого зростання кількості цифрових даних та підвищення залежності бізнес-процесів від інформаційних ресурсів питання їхнього захисту набуває особливої важливості. Витоки конфіденційної інформації можуть призвести до фінансових збитків, репутаційних втрат і порушення нормативних вимог, що робить проблему забезпечення надійного контролю за обробкою та передаванням даних критичною для будь-якої організації.

З огляду на це впровадження технологій захисту від витоку даних на основі DLP-систем є необхідною умовою побудови сучасної ефективної системи інформаційної безпеки. DLP-рішення дозволяють контролювати рух даних, запобігати несанкціонованим передачам та підвищувати рівень відповідності стандартам захисту інформації. Саме тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було визначено зміст проблеми захисту конфіденційних даних в умовах сучасних цифрових загроз, сформульовано мету, завдання та структурні елементи системи запобігання витокам інформації.
2. Досліджено методи та інструменти запобігання витоку даних із застосуванням програмних рішень ManageEngine, а також їх функціональні можливості щодо контролю та моніторингу обробки інформації.
3. Розглянуто структуру та принципи роботи технології DLP на базі ManageEngine, наведено рекомендації щодо її впровадження та налаштування в організаціях різних масштабів.
4. Матеріал подано послідовно та грамотно, висновки сформульовано чітко й аргументовано, а графічні та аналітичні елементи оформлено якісно; список використаних джерел демонструє вміння працювати з фаховою літературою за тематикою інформаційної безпеки.

Недоліки:

1. У кваліфікаційній роботі дослідження проводилося на демонстраційній конфігурації, що не дозволяє повністю врахувати можливі виклики, пов'язані з масштабуванням, навантаженням та взаємодією з іншими системами безпеки всередині організації.
2. У кваліфікаційній роботі не було здійснено практичної інтеграції ManageEngine Endpoint DLP у реальну корпоративну інфраструктуру, що обмежує можливість оцінити поведінку системи у складних середовищах з різними рівнями доступу та розподіленою структурою користувачів.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку “добре”, а здобувач(ка) **БЕЗПРОЗВАННИЙ Михайло** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь,
вчене звання)

(підпис)

(ім'я, прізвище)

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

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється здобувач БЕЗПРОЗВАННИЙ Михайло до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Розробка технології захисту даних в організації на основі DLP».
Кваліфікаційна робота і рецензія додаються.

Директор інституту

(підпис)

Євгенія ІВАНЧЕНКО

(ім'я, прізвище)

Висновок керівника кваліфікаційної роботи

Здобувач **БЕЗПРОЗВАННИЙ Михайло** обрав тему роботи, метою якої було дослідити причини витоків інформації в організації та методи боротьби з ними на основі DLP-рішень, а також розробити рекомендації щодо імплементації DLP-рішення в рамки організації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи **БЕЗПРОЗВАННИЙ Михайло** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **БЕЗПРОЗВАННОГО Михайла** на оцінку “добре” та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи

(підпис)

Євген ПЕДЧЕНКО

(ім'я, прізвище)

“ ” 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БЕЗПРОЗВАННИЙ Михайло** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки

(назва)

(підпис)

Галина ГАЙДУР

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 74 сторінки, рисунків, 1 таблиця, 12 джерел.

Об'єкт дослідження – процес забезпечення захисту конфіденційних даних та упередження їх витоку в організації.

Предмет дослідження – технологія запобігання витоку даних на основі DLP-рішень ManageEngine.

Мета роботи – розробити технологію захисту даних в організації з використанням DLP-системи ManageEngine та сформулювати рекомендації щодо її впровадження й практичного застосування.

Методи дослідження – аналіз фахової літератури та нормативних документів, порівняння технічних характеристик DLP-рішень, дослідження функціональних можливостей ManageEngine Endpoint DLP, моделювання політик контролю даних.

DLP-технології забезпечують комплексний контроль над внутрішніми й зовнішніми потоками інформації, дозволяючи організаціям своєчасно виявляти та блокувати спроби несанкціонованого передавання конфіденційних даних. Рішення ManageEngine Endpoint DLP включає інструменти класифікації інформації, контроль дій користувачів, моніторинг пристроїв та мережевих каналів, аналіз ризиків і гнучке налаштування політик безпеки для запобігання витокам критичних даних.

У роботі розглянуто проблематику витоку інформації в сучасних організаціях, сформульовано мету та основні завдання дослідження. Проведено аналіз підходів і технологій захисту даних, досліджено функціональні можливості DLP-систем, зокрема ManageEngine. Визначено структуру, компоненти та ключові механізми роботи цього рішення.

На основі отриманих результатів розроблено технологію застосування DLP-рішення ManageEngine для захисту даних в організації. Сформовано рекомендації щодо проектування політик безпеки, розгортання, налаштування контролю каналів передачі інформації та подальшої експлуатації системи.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЗАХИСТ ДАНИХ, ВИТІК ІНФОРМАЦІЇ, DLP, MANAGEENGINE, ІНФОРМАЦІЙНА БЕЗПЕКА, КОНТРОЛЬ ДАНИХ, ПОЛІТИКИ БЕЗПЕКИ.

ABSTRACT

Text part of the qualification work: pages, figures, table, 12 sources.

Object of research – the process of protecting confidential data and preventing information leakage within an organization.

Subject of research – the data loss prevention technology based on ManageEngine DLP solutions.

The aim of research – to develop a data protection technology for an organization using the ManageEngine DLP system and to formulate recommendations for its implementation and practical use.

Research methods – analysis of professional literature and regulatory documents, comparison of technical characteristics of DLP solutions, examination of the functional capabilities of ManageEngine Endpoint DLP, and modeling of data control policies.

DLP technologies provide comprehensive control over internal and external data flows, enabling organizations to promptly detect and block attempts of unauthorized transmission of confidential information. The ManageEngine Endpoint DLP solution includes tools for data classification, user activity monitoring, device and network control, risk assessment, and flexible configuration of security policies to prevent leakage of critical information. The paper examines the problem of information leakage in modern organizations, formulates the purpose and key objectives of the research. An analysis of approaches and technologies for data protection is conducted, along with a study of DLP system capabilities, particularly ManageEngine. The structure, components, and key operational mechanisms of the solution are defined. Based on the obtained results, a technology for applying the ManageEngine DLP solution to protect organizational data is developed. Recommendations are provided regarding the design of security policies, deployment, configuration of data transfer channel control, and further system operation.

Field of application – cybersecurity of an organization's information resources.

DATA PROTECTION, INFORMATION LEAKAGE, DLP, MANAGEENGINE,
INFORMATION SECURITY, DATA CONTROL, SECURITY POLICIES.

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В ОРГАНІЗАЦІЇ ТА РОЛІ DLP РІШЕНЬ.....	12
1.1 Дослідження проблеми витоку даних в організації.....	12
1.2 Аналіз підходів до захисту даних від витоку.....	19
1.3 Аналіз існуючих рішень для запобігання витоку даних в організації	27
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ НА БАЗІ СУЧАСНОГО DLP РІШЕННЯ	55
2.1 Призначення та основні функції рішень DLP	55
2.2 Основні компоненти загальної архітектури DLP	67
2.3 Технології Data Classification у DLP системах.....	78
3 ТЕХНОЛОГІЯ ЗАХИСТУ ДАНИХ НА ОСНОВІ DLP РІШЕННЯ	83
3.1 Проектування архітектури впровадження DLP-системи ManageEngine в організації.....	83
3.2 Налаштування політик контролю даних та класифікації у ManageEngine Endpoint DLP.....	86
3.3 Контроль каналів передачі даних та моніторинг інцидентів витоку в ManageEngine Endpoint DLP.....	98
3.4 Рекомендації щодо впровадження, оптимізації та експлуатації DLP-системи в організації.....	
ВИСНОВКИ	102
ПЕРЕЛІК ПОСИЛАНЬ	105
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	106

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

IAM – Identity and Access Management

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

MFA – Multi-Factor Authentication

SIEM – Security Information and Event Management

UEBA – User and Entity Behavior Analytics

VPN – Virtual Private Network

AES – Advanced Encryption Standard

SSL/TLS – Secure Sockets Layer / Transport Layer Security

CASB – Cloud Access Security Broker

ACL – Access Control List

CSP – Cloud Service Provider

API – Application Programming Interface

SOC – Security Operations Center

POC – Proof of Concept

KPI – Key Performance Indicator

CSV – Comma-Separated Values

REST – Representational State Transfer

JSON – JavaScript Object Notation

TLS – Transport Layer Security

SMTP – Simple Mail Transfer Protocol

DDoS – Distributed Denial of Service

RBAC – Role-Based Access Control

PKI – Public Key Infrastructure

ВСТУП

Актуальність дослідження. У сучасних умовах цифрової трансформації організації оперують дедалі більшими обсягами конфіденційних даних, що циркулюють між внутрішніми інформаційними системами, хмарними сервісами, кінцевими пристроями та зовнішніми комунікаційними каналами. Розвиток віддаленої роботи, використання персональних пристроїв, активний обмін інформацією через мережеві сервіси та підвищення мобільності працівників посилюють ризики витоку даних. У таких умовах традиційні моделі периметрової безпеки втрачають ефективність, оскільки вони не здатні забезпечити контроль над даними незалежно від середовища їх обробки чи переміщення.

Зростання рівня кіберзагроз, поява складних атак, внутрішні інциденти, помилки персоналу та навмисні дії зловмисників змушують організації впроваджувати інтелектуальні системи контролю даних. Зокрема, технології Data Loss Prevention (DLP) стають ключовим елементом сучасних концепцій інформаційної безпеки. Вони забезпечують моніторинг, виявлення, блокування та попередження витоків даних у режимі реального часу, дозволяючи організаціям контролювати весь життєвий цикл інформації.

Розглянуте DLP-рішення ManageEngine Endpoint DLP пропонує комплексний підхід до запобігання витоку даних завдяки поєднанню класифікації інформації, політик доступу, контролю пристроїв, моніторингу мережевих каналів, поведінкового аналізу та реагування на інциденти. Гнучкість його налаштувань дозволяє адаптувати механізми захисту під потреби організацій різних масштабів і сфер діяльності.

Враховуючи критичну важливість контролю даних для забезпечення стійкості бізнес-процесів, а також актуальні вимоги міжнародних стандартів та регуляторних норм, дослідження технології захисту даних на основі DLP-систем, зокрема ManageEngine, є своєчасним, науково обґрунтованим та практично значущим.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології забезпечення мінімізування витоків даних організації поза її межі на базі ManageEngine DLP.

Об'єкт дослідження – процес забезпечення захисту конфіденційних даних та запобігання їх витоку в організації.

Предмет дослідження – технологія захисту даних на основі DLP-рішень ManageEngine.

Мета роботи – розробити технологію застосування DLP-системи ManageEngine для захисту даних в організації та сформулювати рекомендації щодо її впровадження і подальшої експлуатації.

Наукові завдання:

- дослідити сутність проблеми витоку даних в організації;
- проаналізувати існуючі підходи та методи захисту інформації від витоку;
- дослідити сучасні DLP-рішення та їх функціональні можливості;
- проаналізувати механізми і компоненти DLP-системи ManageEngine;
- розробити технологію впровадження DLP-рішення ManageEngine та порядок побудови політик безпеки;
- сформулювати рекомендації щодо застосування DLP для забезпечення ефективного контролю даних.

Методи дослідження – Опрацювання фахової літератури, аналіз нормативно-правових документів, порівняння технічних характеристик сучасних DLP-систем, дослідження функціональних можливостей ManageEngine Endpoint DLP, моделювання політик безпеки та оцінка ризиків витоку даних.

Практичне значення одержаних результатів: У роботі запропоновано технологію впровадження DLP-рішення ManageEngine в інформаційну інфраструктуру організації, розроблено рекомендації щодо створення політик контролю даних, налаштування моніторингу каналів передачі інформації та організації реагування на інциденти. Отримані результати можуть бути використані фахівцями з кібербезпеки для підвищення рівня захисту інформаційних ресурсів підприємств різних галузей.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В ОРГАНІЗАЦІЇ ТА РОЛІ DLP РІШЕНЬ

1.1. Дослідження проблеми витоку даних в організації

Цифрові інновації, масштабна цифровізація бізнес-процесів, розвиток хмарних сервісів і перехід організацій до гібридних форм роботи докорінно змінили сучасне інформаційне середовище. У цих умовах дані стали не просто елементом операційної діяльності, а ключовим стратегічним активом, від збереження якого залежить конкурентоспроможність, фінансова стабільність і репутація організації. Проте одночасно з розширенням цифрової інфраструктури суттєво зросла й кількість загроз, пов'язаних із несанкціонованим розголошенням, переміщенням або втратою конфіденційної інформації. Саме тому проблема витоку даних стала однією з найактуальніших у сфері інформаційної та кібербезпеки, а запобігання цьому явищу визначило попит на комплексні технології класу Data Loss Prevention (DLP).

Витік даних — це несанкціоноване розкриття, передавання, копіювання або доступ до конфіденційної інформації, що призводить до її потрапляння до осіб чи систем, які не мають законних прав на її отримання. Сутність цього явища полягає в порушенні одного або кількох базових принципів інформаційної безпеки — конфіденційності, цілісності та доступності (CIA-тріади), але найчастіше страждає саме конфіденційність. Під витоком розуміють не лише публічне оприлюднення даних, але й будь-який факт неконтрольованого переміщення інформації за межі дозволеного периметра, у тому числі випадкову передачу даних, копіювання на незахищений носій або некоректне налаштування доступів.

Сутність витоку даних полягає в тому, що інформація втрачає контрольованість: організація більше не може повністю визначати, де вона зберігається, хто її читає, у якій формі вона використовується і чи не була змінена. У сучасному цифровому середовищі це створює значні ризики: від фінансових втрат і прямої шкоди бізнесу до репутаційних криз та юридичної

відповідальності відповідно до норм GDPR, HIPAA, PCI DSS та інших законодавчих актів.

Особливістю сучасних витоків є те, що вони відбуваються навіть у присутності розвиненої системи захисту периметра. Класичні інструменти, такі як брандмауери або антивірусні рішення, орієнтовані на зовнішні загрози, тоді як значна частина витоків відбувається всередині організації або поза її фізичним периметром, коли співробітники використовують хмарні сервіси, особисті пристрої чи віддалено підключаються до корпоративних ресурсів.

Однак масштаби та характер витоків інформації дедалі змінюються: вони можуть бути спричинені не лише зовнішніми атаками, а й внутрішніми помилками, технічними недоліками, неправильно налаштованими хмарними службами чи поєднанням багатьох факторів. Така багатофакторність робить проблему витоків даних надзвичайно складною та актуальною.

Організаційна цифровізація, хмарні сервіси, віддалена робота та BYOD-моделі розширили кількість каналів, через які інформація може бути випадково або навмисно виведена з-під контролю. Аналітичні звіти свідчать, що витoki стають дорожчими й складнішими: середня вартість інциденту у 2023 році досягла близько 4,45 млн USD, а час виявлення та локалізації інцидентів часто вимірюється місяцями, що підсилює шкоду й ускладнює реагування [1]. У такій ситуації ключовим є розуміння класифікації причин витоків — адже лише так можна вибудувати ефективну стратегію превенції та технологічної відповіді.

У контексті дослідження проблеми витоків даних важливо не лише розглядати загрозу в цілому, а й розуміти, які саме категорії інформації є критичними для організації. До таких, зокрема, належать: персональні дані клієнтів і співробітників (у тому числі спеціальні категорії персональних даних), фінансові та платіжні реквізити, комерційні таємниці (бізнес-стратегії, плани розвитку, маркетингові дослідження), інтелектуальна власність (вихідний код, технічна документація, результати НДР), а також службова інформація обмеженого доступу. Для кожного типу даних характерні різні сценарії використання, різний рівень чутливості й різна регуляторна відповідальність.

Тому в межах сучасних моделей управління інформаційною безпекою особливу увагу приділяють класифікації даних і присвоєнню їм відповідних рівнів критичності та міток доступу, що згодом визначає, які саме технічні й організаційні контролі мають бути застосовані до конкретних інформаційних активів.

Людський фактор і ненавмисні помилки залишаються одними з найбільш поширених причин інцидентів. Працівники можуть випадково відправити конфіденційний документ не тій людині, синхронізувати робочі папки з особистими хмарними акаунтами або скопіювати інформацію на незашифровані зовнішні накопичувачі. Часто такі дії не мають злого умислу, але їхні наслідки можуть бути катастрофічними. Наприклад, безліч бізнесів зазнали втрат через те, що співробітники пересилали або викладали в мережу внутрішні файли, не усвідомлюючи ризиків; у таких випадках заходи навчання та жорсткі політики контролю доступу могли б мінімізувати шкоду. Загальні дослідження підтверджують, що людський чинник бере участь в дуже великому відсотку інцидентів і часто поєднується з іншими факторами, тому рішення повинні включати культуру безпеки, навчання і технічні обмеження, які роблять випадкові дії менш ризикованими [2].

Інсайдерські загрози (навмисні дії співробітників або підрядників) становлять окрему і надзвичайно небезпечну категорію. Інсайдери мають легальний доступ до ресурсів і знають бізнес-процеси та місця зберігання даних, що дає їм можливість обходити базові механізми захисту. Історичні кейси демонструють це чітко: так, випадок із технічним персоналом, який викрадав і передавав вихідний код або комерційні тайни, показав, що відсутність моніторингу дій користувачів і недостатня сегментація доступів створює передумови для масштабних витоків — у таких інцидентах критична роль належить не лише виявленню факту витоку, а й аудиту й можливості відкотити наслідки [3].

Технічні вразливості й конфігураційні помилки — ще одна поширена причина. Інфраструктура, яка не оновлюється вчасно або неправильно

налаштована, відкриває «вхідні двері» для зловмисників. Класичний і трагічний приклад — Equifax (2017): компанія не встановила доступний патч для вразливості Apache Struts (CVE-2017-5638), внаслідок чого були викрадені персональні дані приблизно 143 млн осіб; цей інцидент показав, як проста конфігураційна та процесна недбалість призводить до катастрофи [4]. Інша велика категорія таких помилок — неправильні налаштування хмарних ресурсів (відкриті S3-пляшки, надмірні права доступу), що призвели до масових випадків викриття даних у різних організаціях; прикладом є низка інцидентів, коли конфігураційні помилки в AWS або інших CSP ставали доступними через public buckets або некоректні SAS-токени, як це сталося у випадку великого витoku Microsoft (2023), коли помилка в SAS-токені дозволила експонувати десятки терабайт даних [5][6]. Ці події підтверджують необхідність уважного процесного підходу до конфігурацій і автоматичного валідування безпечних налаштувань.

Зовнішні атаки — фішинг, крадіжка облікових даних, шкідливе ПЗ і supply-chain-атаки — регулярно призводять до серйозних витоків. Приклад SolarWinds (2020) яскраво ілюструє ризики ланцюга постачальників: шкідливий код був інжектований в оновлення Orion, і більше 18 000 клієнтів опинилися під загрозою, включно з урядовими установами та великими корпораціями; цей випадок показав, що компрометація одного постачальника може піддати ризику численні організації й призвести до витoku внутрішніх даних клієнтів [7]. Подібно, у 2019 році витік у Capital One виник через експлуатацію неправильно налаштованого веб-взаємодії з хмарними сервісами — зловмисник скористався помилкою в конфігурації і отримав доступ до даних понад 100 мільйонів осіб у США й Канаді [8]. У 2023 році уразливість у MOVEit призвела до численних витоків в результаті експлуатації вразливості в MFT-продукті: десятки тисяч організацій постраждали, було скомпрометовано десятки мільйонів записів, що підкреслило вразливість централізованих механізмів обміну файлами [9][10].

Хмарні сервіси та API-інтеграції часто створюють «темні зони» видимості: дані можуть переміщуватися між SaaS-додатками, обмінюватися через сторонні інструменти, і при цьому традиційні засоби периметрового захисту не фіксують

таких потоків. Помилкові публічні конфігурації, надмірні ролі чи API-ключі з широкими правами — усе це дає шлях до витоків без явного вторгнення.

Наприклад, прогалини у налаштуваннях публічних сховищ та уразливості в програмах передачі файлів призвели до того, що за низкою інцидентів інформація стала доступною публічно або опинилася в руках кіберзлочинців через автоматизовану ексфільтрацію [6][9].

Неконтрольовані канали — USB-носії, приватні пристрої, месенджери та соціальні мережі — також відіграють значну роль у витоках. Навіть якщо внутрішні системи контролю працюють, працівник може скопіювати файл на флешку або надіслати його через особистий Gmail або Telegram; це одна з причин, чому політики BYOD і контроль кінцевих точок стають критично важливими. Багато гучних розслідувань виявили, що саме такі «ручні» операції спричиняли масштабні витoki, оскільки системи моніторингу не охоплювали приватні канали або не мали правил для поведінки користувачів у хмарі чи через особисті сервіси. У галузі охорони здоров'я ефективним прикладом є досвід *Mayo Clinic*. Велика кількість лікарів та медичних працівників працює дистанційно або використовує мобільні пристрої. Після впровадження мобільного DLP стало можливим контролювати передачу медичних документів, зображень та PDF-файлів. Система почала автоматично блокувати спроби надсилання медичних знімків через неавторизовані месенджери та виявляти нестандартні операції експорту даних. Це значно знизило ризики витоку персональних медичних даних, що є критичним при дотриманні HIPAA.

Якщо розглядати витік даних з погляду каналів, то в більшості організацій виділяють кілька ключових груп. По-перше, це електронна пошта та веб-канали (веб-форми, особисті хмарні сховища, веб-пошта), які часто використовуються як для повсякденної роботи, так і для несвідомого або навмисного виведення інформації за межі корпоративного периметра. По-друге, це файлові протоколи та сервіси обміну (FTP/SFTP, MFT-рішення, внутрішні файлові шари, системи спільного доступу до документів), через які відбуваються як легітимні бізнес-процеси, так і прихована ексфільтрація. По-третє, канали друку і фізичні носії

(принтери, сканери, USB-накопичувачі, зовнішні диски), де цифровий контроль часто слабший, а виявлення інцидентів складніше. Окрему категорію становлять сучасні комунікаційні платформи — корпоративні та публічні месенджери, VoIP, засоби для відеоконференцій, інтегровані з обміном файлами. Саме така багатоманітність каналів робить традиційні підходи, що спираються винятково на захист периметра, недостатніми і підкреслює необхідність систем, здатних аналізувати вміст і контекст передавання даних у різних середовищах у режимі, наближеному до реального часу.

Ще одна важлива складова — відсутність або слабкість управлінських процесів: недостатнє сегментування мережі, відсутність принципу найменших привілеїв (*least privilege*), недостатній аудит доступів і логування дій користувачів. Історія показує, що якщо права користувачів надмірні або контролю відсутні, знайти та зупинити інсайдерську атаку або зовнішню експлуатацію вразливості стає набагато складніше. Приклад Target (2013) — компрометація через обліковий запис підрядника без належних обмежень — демонструє, як слабкі організаційні межі і відсутність сегментації створюють умови для масового витоку платіжних даних [11].

Статистично, звіти Verizon і IBM підтверджують тренди, що поєднують людські, технічні та постачальницькі фактори. Verizon DBIR 2023 вказує, що великою часткою джерел атак залишаються зовнішні актори (понад 80 %), але роль людського елемента (фішинг, помилки) також залишається дуже високою [2]. IBM Cost of a Data Breach Report 2023 підкреслює збільшення середніх витрат і тривалості інцидентів, що робить раннє виявлення та запобігання особливо цінними — саме в цьому полі DLP-інструменти показують свою економічну обґрунтованість, оскільки вони можуть знизити ризик ексфільтрації й скоротити час до реагування [1].

Ускладнення, що виникають після витоку даних, проявляються на кількох рівнях — фінансовому, операційному, репутаційному та регуляторно-правовому. Згідно зі сучасними дослідженнями, середня глобальна вартість одного порушення безпеки даних сьогодні сягає майже п'яти мільйонів доларів США. Це

включає прямі фінансові збитки, втрату доходів, витрати на відновлення операцій, компенсації та підтримку клієнтів. Особливо суттєвими є витрати на реагування: цифровий форензик, зовнішні консалтингові послуги, роботу служб підтримки, юридичний супровід та обов'язкові процедури інформування постраждалих осіб.

Найбільших збитків зазнають ті галузі, які працюють із медичними, фінансовими чи іншими високочутливими даними. У сфері охорони здоров'я середня вартість інциденту є майже вдвічі вищою, ніж у середньому по ринку, а витік медичних записів часто тягне за собою не лише фінансові витрати, а й значні юридичні наслідки. Близько 70 % організацій, які зіткнулися з витоком, повідомляють про суттєві порушення бізнес-процесів: збої в роботі інформаційних систем, призупинення сервісів, необхідність термінового перерозподілу ресурсів, перевипуск облікових даних та зміну процесів взаємодії з клієнтами.

Регуляторні наслідки також стають однією з найвитратніших частин інциденту. У багатьох країнах законодавство зобов'язує організації повідомляти про витоки персональних даних, а недотримання цих вимог карається штрафами. Крім того, компанії можуть стикатися з колективними позовами клієнтів та партнерів, що значно збільшує фінансовий тиск та репутаційні ризики. Навіть якщо витік не спричинив негайної фінансової шкоди, тривалий негативний імідж у медіапросторі впливає на довіру, відтік клієнтів, падіння капіталізації та складнощі з укладанням нових контрактів. Відновлення репутації часто вимагає тривалих PR-кампаній, підвищених гарантій безпеки та зміни підходів до роботи з клієнтами.

Ще один вагомий наслідок — зростання витрат на кібербезпеку після інциденту. Компанії змушені інвестувати у модернізацію IT-інфраструктури, впровадження нових інструментів, розбудову систем моніторингу, навчання працівників та регулярне тестування на проникнення. Попри те що це збільшує загальні витрати, статистика показує: організації, які активно застосовують автоматизацію процесів безпеки та мають сформований план реагування на інциденти, знижують сумарну вартість витоку в середньому на декілька мільйонів

доларів порівняно з тими, хто покладається лише на базові механізми захисту.

З огляду на складність і багатофакторність причин витоку даних, сучасний підхід до їхнього запобігання ґрунтується не на окремих технічних продуктах, а на побудові цілісної системи управління інформаційними ризиками. У її межах поєднуються політики безпеки, процеси управління доступом і привілеями, класифікація й інвентаризація даних, моніторинг інфраструктури та поведінки користувачів, регулярний аудит і навчання персоналу. Технології захисту — такі як засоби керування ідентичностями (IAM), системи журналювання та кореляції подій (SIEM), рішення для захисту хмарних сервісів (CASB), засоби шифрування — доповнюють одна одну. DLP-системи в цій екосистемі відіграють особливу роль, оскільки вони фокусуються безпосередньо на контролі руху даних, їхньому вмісті та контексті використання, дозволяючи виявляти і блокувати спроби ексфільтрації як через традиційні, так і через нетипові канали. Саме інтеграція DLP-рішень у загальну архітектуру безпеки дає можливість перейти від реактивного до превентивного підходу, коли ризик витоку знижується вже на етапі проєктування бізнес-процесів і IT-систем.

Усі ці фактори — прямі фінансові втрати, юридичні та репутаційні ризики, операційні збої, підвищення витрат на IT та безпеку — демонструють, що витік даних є однією з найнебезпечніших загроз для сучасної організації. Позаяк дані стають ключовим активом, здатним визначати конкурентоспроможність та стійкість бізнесу, увага до їх захисту набуває стратегічного значення. Саме тому системи класу DLP мають критично важливу роль: вони забезпечують контроль над переміщенням, копіюванням і передаванням даних, блокують несанкціоновані дії, аналізують поведінку користувачів, унеможлиблюють використання небезпечних каналів та забезпечують швидке реагування на інциденти ще до того, як відбудеться фактичний витік.

Тож витік даних перестає бути суто технічним інцидентом — він перетворюється на комплексну кризу, здатну вплинути на фінансову стабільність, репутацію та розвиток організації. А захист інформації стає фундаментальним елементом побудови стійкої, зрілої та захищеної кібербезпекової архітектури.

1.2. Аналіз підходів до захисту даних від витоку

Проблема витоку даних вимагає застосування різноманітних підходів, які враховують складність цифрового середовища та багатоаспектність сучасних інформаційних систем. У міру того як організації переходять до моделі «дані всюди» (data everywhere), класичні методи безпеки поступово втрачають ефективність. Доступ до корпоративних ресурсів відбувається з різних локацій, через різні мережі, з особистих і корпоративних пристроїв, через хмари, API, сторонні сервіси, мобільні застосунки та розподілені системи зберігання. Тому підхід до захисту даних уже не може ґрунтуватися лише на периметрі або статичних правилах доступу — він має бути глибоко інтегрованим у саму природу інформаційних потоків.

Одним з фундаментальних напрямів сучасного захисту є концепція Data-Centric Security — безпека, орієнтована на самі дані, а не на інфраструктуру. На відміну від традиційної моделі, де акцент робився на захисті мережевих сегментів і кінцевих вузлів, сучасні підходи зосереджуються на класифікації, контролі, стеженні та управлінні інформаційними активами протягом усього їхнього життєвого циклу. У цьому контексті DLP-системи стають центральним інструментом, оскільки вони контролюють операції з даними незалежно від того, де вони знаходяться: у хмарі, локально, на смартфоні, у веб-застосунку чи під час передавання між внутрішніми і зовнішніми системами.

Захист від витоку даних сьогодні реалізується шляхом поєднання кількох ключових методів. Один із них — політики доступу, побудовані на принципах Zero Trust. У рамках Zero Trust кожен запит на доступ до інформації розглядається як недостовірний доти, доки його не буде перевірено. Це означає, що навіть авторизований співробітник повинен підтвердити свою ідентичність, контекст роботи та безпечність свого середовища кожного разу, коли намагається працювати з чутливими даними. Такі підходи мінімізують ризик того, що компрометований обліковий запис або скомпрометований пристрій призведе до масового витоку. Одним з найбільш показових прикладів ефективності

адаптивних політик доступу є досвід компанії *ING Group*. Банк впровадив модель Zero Trust ще у 2021 році, поєднавши її з централізованими DLP-політиками та автоматичним аналізом контексту. Після інтеграції поведінкової аналітики система почала фіксувати нетипові операції співробітників — наприклад, копіювання великої кількості даних у позаробочий час. Зафіксований інцидент, який раніше міг би залишитися непоміченим, був автоматично заблокований, а система DLP ізолювала робочу станцію. За оцінками служби безпеки ING, саме поєднання Zero Trust + поведінкова аналітика дозволило запобігти потенційному масовому витоку фінансової інформації.

Серед ключових підходів до запобігання витоку даних особливе місце займає класифікація інформації. Без чіткого розуміння того, які дані є конфіденційними, критичними чи публічними, неможливо побудувати ефективні політики контролю. Сучасні DLP-рішення інтегрують автоматичну класифікацію на основі машинного навчання: система аналізує структуру документа, ключові слова, шаблони й історію використання файлу для того, щоб присвоїти йому мітку чутливості. Це дає можливість автоматично застосовувати до документа політики доступу, шифрування, моніторингу та обмеження передачі. Не менш показовим є кейс компанії *Siemens*, яка активно використовує класифікацію даних як основу своєї політики безпеки. На початку 2022 року Siemens оновила глобальні політики Data Governance, впровадивши автоматичну класифікацію всіх документів із застосуванням ML-алгоритмів. Це дало можливість системі відразу позначати креслення, патенти, технологічні процеси та документацію рівнем «висока конфіденційність». Результатом стало різке зменшення обсягів критичних даних, які помилково надсилалися партнерам через звичайну електронну пошту. За перший рік кількість випадкових витоків через неправильну класифікацію знизилася більш ніж на 70 %. Цей кейс демонструє, що навіть у компаніях з високою технологічною культурою класифікація відіграє ключову роль у запобіганні інцидентам.

Класифікація також дозволяє реалізовувати моделі Data Tagging та Data Labeling, коли інформація супроводжується метаданими про чутливість. Це

надзвичайно важливо в масштабних організаціях, де документи передаються між різними системами. У таких умовах DLP може відстежувати переміщення інформаційних блоків навіть у складних структурах — у вкладених файлах, зашифрованих архівах, імпортованих таблицях та API-запитах. У промисловому секторі одним із найкращих прикладів успішного застосування DLP-підходів є компанія *Schneider Electric*. Величезна кількість проєктної документації, креслень та інтелектуальної власності циркулює між підрозділами всередині компанії та зовнішніми підрядниками. У 2022 році *Schneider* інтегрувала спеціалізовану DLP-систему з інструментами PLM. Виявилося, що понад 8 % усіх документів передавалися партнерам без відповідних рівнів шифрування або класифікації. Після впровадження централізованого контролю компанія скоротила кількість ризикових передач інформації на 90 %, а сама система почала автоматично застосовувати шифрування на основі тегів конфіденційності.

Другим важливим напрямом є шифрування. Хоча шифрування саме по собі не запобігає крадіжці даних, воно робить украдену інформацію практично непридатною для використання. Сучасні підходи до шифрування включають політики автоматичного шифрування конфіденційних документів при переміщенні через ненадійні канали або при зберіганні на портативних носіях. Низка організацій застосовує селективне шифрування, коли файлові системи шифруються на рівні окремих об'єктів з різними ключами залежно від призначення файлу. Інші використовують токенізацію — заміну реальних даних на псевдоніми, що робить їх непридатними для злоумисників навіть у разі витоку.

Ключовим підходом до зниження ризику витоку є управління правами та привілеями (PAM, IAM). Контроль привілеїв дозволяє чітко визначити, які користувачі можуть працювати з певною інформацією, і в яких умовах. Модель *least privilege* передбачає, що співробітник отримує лише ті права, які необхідні йому для виконання конкретних робочих задач. На практиці це означає, що навіть співробітники високого рівня не мають доступу до всіх даних, а права коригуються залежно від ситуації. DLP-рішення у цьому контексті стають інструментом перевірки дотримання політик доступу: система фіксує всі спроби

отримання інформації, аналізує їх та блокує у разі порушення принципів мінімально необхідних привілеїв.

Сегментація мережі — ще один стратегічний підхід. Він полягає у розділенні інфраструктури на декілька ізольованих сегментів, між якими існують жорсткі правила доступу. Якщо зломисник проникає до одного сегмента, він не може автоматично отримати доступ до всіх інших. Це обмежує масштаб потенційного витоку та дає час на його виявлення. Сегментація також підтримує політику Zero Trust і тісно інтегрується з DLP-системами, що дозволяє будувати горизонтальні бар'єри навіть всередині одного підрозділу.

Дуже важливою складовою підходів до захисту є контроль кінцевих точок. Сучасні робочі станції мають широкий набір каналів, які можуть використовуватися для ексфільтрації даних: USB, Bluetooth, AirDrop, локальні архіватори, віртуальні принтери, буфер обміну, VPN-клієнти, браузері, месенджери, хмарні файлові менеджери. У межах цього напрямку DLP-рішення забезпечують моніторинг будь-яких операцій копіювання, передавання, архівування, друку та завантаження. Control-over-clipboard, print-screen-detection, USB device blocking, dynamic rules for shadow copies — усе це частини сучасного кінцевого захисту. У сфері контролю кінцевих точок яскравим прикладом є досвід *Deloitte*. Після впровадження комплексної системи контролю USB-носіїв *Deloitte* виявила, що понад 40 % співробітників намагалися переносити робочі файли на зовнішні накопичувачі. Частина цих дій була ненавмисною (зручність роботи поза офісом), а частина — порушенням політик. Endpoint DLP заблокувала подібні запити, і за підсумками аудиту було встановлено, що без цих рішень існував би постійний ризик витоку конфіденційних даних клієнтів. Водночас *Deloitte* впровадила зашифровані «білі» носії лише для обмеженого числа департаментів, що стало прикладом практичного впровадження моделі least privilege.

Суттєвим підходом є виявлення аномалій та аналіз поведінки. Поведінкові моделі дають змогу визначати нетипові дії: раптове масове копіювання файлів, доступ до нетипових директорій, завантаження великої кількості документів у нічний час, перенесення конфіденційної інформації на зовнішні сервіси. Такі

системи формують профілі нормальної поведінки та повідомляють про відхилення. У звітах зазначається, що поведінкові алгоритми дозволяють зменшити шкоду від інсайдерських інцидентів у середньому на третину, оскільки вони фіксують підозрілу активність до того, як відбудеться фактичний витік. Хорошим прикладом ефективності адаптивних політик та поведінкової аналітики є кейс UBS Bank. У 2023 році співробітник банку намагався завантажити понад 1 200 файлів на свій особистий Google Drive після зміни ролі всередині компанії. Система DLP не тільки заблокувала дію, але й автоматично ідентифікувала це як відхилення від типової поведінки користувача, повідомила службу безпеки та запустила внутрішній розслідувальний процес. За оцінками UBS, це запобігло можливому витoku інформації, яка відносилася до сегменту високочутливих операційних документів банку.

Сучасна статистика свідчить, що значна частина витоків пов'язана з неправильними конфігураціями хмарних сервісів. За даними світових звітів, понад 80 % організацій хоча б один раз за останні роки мали інцидент у хмарі через помилкові налаштування. До цього належать відкриті сховища, неправильно налаштовані API-ключі, публічні посилання на внутрішні документи, надмірні права користувачів і сторонніх застосунків. У цих умовах хмарні DLP-рішення стають незамінними, оскільки вони аналізують політики доступу в реальному часі та обмежують потенційно небезпечні операції. Компанія *Dropbox Business* упродовж останніх років активно використовує Cloud DLP у поєднанні з CASB-рішеннями. Після впровадження повноцінного контролю API-запитів було ліквідовано понад 12 000 публічних посилань на внутрішні файли, які співробітники створювали помилково або через незнання політик. У кількох окремих випадках потенційно конфіденційні документи з технічної документації були доступні за зовнішнім посиланням, однак DLP-система автоматично помітила аномальне створення такої лінки та заблокувала її до того, як її побачили сторонні користувачі.

Для забезпечення високого рівня захисту даних необхідно також впроваджувати підходи до регулярного моніторингу та реагування на інциденти.

DLP інтегрується з системами SIEM та SOAR, які уможливають автоматизоване реагування. Якщо система виявляє спробу передачі конфіденційного файлу через заборонений канал, вона може не лише заблокувати дію, а й запустити сценарій реагування: повідомити службу безпеки, призупинити обліковий запис, зібрати журнал подій та почати форензичне збереження доказів. Це дозволяє виявляти інциденти вже на ранніх стадіях і зменшувати їхній масштаб. Цікаво відзначити кейс компанії *Zoom*, яка після 2020 року активно перебудовувала свою безпекову інфраструктуру. Зі зростанням кількості корпоративних клієнтів виникла потреба жорстко контролювати записи зустрічей, чати, документи та файли, що передаються через платформу. У процесі впровадження DLP *Zoom* виявила десятки сценаріїв, у яких співробітники могли випадково публікувати внутрішні записи або ділитися конфіденційними файлами через особисті акаунти. DLP-система, інтегрована з хмарною платформою, почала автоматично маркувати записи зустрічей тегами конфіденційності, блокувати зовнішні розшарування та створювати журнал доступу. Завдяки цьому кількість інцидентів із неправильною публікацією записів скоротилася майже до нуля.

Окремою категорією підходів є моделювання загроз. Організації дедалі частіше використовують моделі STRIDE, MITRE ATT&CK, DREAD та інші методології для прогнозування потенційних векторів ексфільтрації. Аналіз векторів, описаних у MITRE (наприклад, Exfiltration Over Web Services, Exfiltration Over Physical Medium), дозволяє формувати точні правила DLP і виявляти навіть нетипові канали передачі, які не входять до стандартних правил безпеки.

Надзвичайно важливою складовою сучасного підходу до захисту даних є навчання персоналу. Незважаючи на складні технології, саме працівники часто є «вхідною точкою» для витоку. Статистичні звіти підтверджують, що більшість інцидентів пов'язана з людським фактором. Тому регулярні тренінги, симуляції фішингових атак, пояснення політик безпеки та оцінка грамотності співробітників стають критично важливими. Практика показує, що організації, де проводять систематичне навчання, зменшують імовірність витоку в декілька разів.

Не менш важливими є й юридичні підходи. Законодавства різних країн вимагають від компаній дотримання певних стандартів щодо захисту персональних та фінансових даних. Регуляторні вимоги (GDPR, HIPAA, CCPA, PCI DSS) накладають обов'язки щодо обмеження доступу, інформування про інциденти, оцінки ризиків і захисту даних. DLP-системи значно полегшують дотримання цих норм, оскільки вони ведуть журнал подій, фіксують інциденти, формують звіти та забезпечують контроль відповідності.

У сучасному цифровому середовищі організації дедалі частіше застосовують підходи до автоматизації безпеки. Це дозволяє значно скоротити час реагування на інциденти. У поєднанні з DLP, автоматизація дає змогу створювати сценарії: якщо файл з міткою «конфіденційно» завантажується на сторонній сервіс, система автоматично блокує запит, надсилає повідомлення адміністратору, запускає аналіз користувача та відновлює політики доступу.

Іншим сучасним підходом є Data Flow Mapping — побудова карти руху інформації в організації. Це дає змогу побачити, як дані проходять через системи, які точки є ризиковими, які канали потребують посилення, де відсутня сегментація або журналювання. DLP у цьому контексті виконує роль датчика, який постачає інформацію про всі транзакції з файлами. Один з наймасштабніших прикладів — впровадження процесів Data Flow Mapping у BP (*British Petroleum*). Корпорація мала складну мережу документообігу між різними географічними офісами. Карта потоків даних виявила низку ланцюгів, де інформація передавалася через застарілі або незахищені засоби обміну файлами. Після інтеграції DLP з процесом мапінгу було знайдено понад 600 неконтрольованих точок передачі інформації. Більшість із них було автоматично закрито, а критичні канали — перенаправлено через захищені платформи.

У деяких організаціях застосовують також підходи до віртуалізації середовища, коли доступ до критичних документів можливий лише у віртуальному робочому столі, де будь-які дії (копіювання, скриншот, передача) суворо контролюються. Це дозволяє мінімізувати ризик витоку через неконтрольовані канали. У великих R&D-центрах особливо поширені методи

боротьби з витоком через скриншоти та екранний запис. Компанія *NVIDIA* реалізувала спеціальну DLP-політику, яка блокує спроби робити скриншоти в захищених середовищах розробки. Після її впровадження кількість спроб ексфільтрації через знімки екрана скоротилася майже повністю. Оскільки корпоративні секрети *NVIDIA* часто пов'язані з інноваційними GPU, нові політики дозволили убезпечити інтелектуальні розробки від інсайдерських загроз.

При інтеграції підходів до захисту даних із загальною стратегією безпеки значну роль відіграє також управління життєвим циклом даних. У цьому аспекті особливо важливо контролювати не лише передавання та зберігання інформації, а й її видалення. Некоректне або неповне видалення файлів — одна з найчастіших причин витоків. DLP-системи забезпечують контроль над цими процесами, ведучи облік усіх копій даних та перевіряючи, чи видаляються вони відповідно до політик.

Узагальнюючи, сучасні підходи до захисту даних охоплюють величезну кількість технічних, організаційних, юридичних і поведінкових методів. У кожному з них DLP займає центральне місце, оскільки саме ці системи здатні забезпечити контроль за рухом даних незалежно від інфраструктури та каналів. DLP виконує роль «нервової системи» безпеки: відстежує взаємодію з даними, аналізує її, фіксує порушення, блокує небезпечні операції та адаптує політики. Завдяки поєднанню контентного аналізу, контекстного моделювання, поведінкової аналітики, роботи з класифікацією й інтеграції з SIEM/SOAR — DLP дозволяє організаціям переходити від реактивного захисту до превентивного, забезпечуючи високу стійкість до інцидентів та відповідність регуляторним вимогам.

1.3. Аналіз існуючих рішень для запобігання витоку даних в організації

У сучасних організаціях управління даними перетворилося на окремий напрям діяльності, що вимагає застосування спеціалізованих технологічних платформ. Якщо в попередніх підрозділах було визначено характер проблеми витоку даних та розглянуто принципові підходи до її запобігання, то подальший

аналіз має на меті оцінити конкретні технологічні рішення, доступні на світовому ринку. Це важливо тому, що на практиці ефективність політик та методів захисту безпосередньо залежить від можливостей інструментів, за допомогою яких вони реалізуються.

Сучасні DLP-рішення значно відрізняються між собою як архітектурою, так і функціональністю, сферою застосування, масштабованістю, складністю впровадження та рівнем автоматизації. Частина рішень орієнтована на великі корпорації з розгалуженою інфраструктурою, інші — на середній бізнес, де ключову роль відіграє баланс між вартістю, простотою адміністрування та достатнім рівнем контролю. Окрему категорію складають хмарні та гібридні платформи, оптимізовані для організацій, що працюють у багатосервісному середовищі та активно інтегрують SaaS-додатки.

Суттєвою відмінністю між рішеннями є також філософія їхньої роботи: одні продукти роблять акцент на глибокому аналізі контенту, інші — на поведінковому профілюванні користувачів, деякі — на розширених можливостях контролю кінцевих точок або хмарних API. Існують рішення, тісно інтегровані з екосистемами Microsoft, Google чи Palo Alto, а також універсальні платформи, які однаково ефективно працюють у гібридних інфраструктурах. Важливо й те, що ринок DLP перебуває під впливом нормативних вимог, які диктують обов'язкові функції для різних секторів — фінансового, медичного, промислового, державного.

Аналіз ринку DLP неможливий без урахування реального досвіду впровадження. Професійні форуми, технічні спільноти, галузеві огляди й звіти аналітичних агентств дозволяють побачити не лише формальні можливості продуктів, але й те, як вони працюють у довгостроковій експлуатації: наскільки стабільно функціонують агенти, які труднощі виникають із налаштуванням політик, які рішення демонструють мінімальну кількість хибних спрацьовувань, а які — потребують значних ресурсів для підтримки. У сукупності це створює реалістичну картину, яка суттєво впливає на вибір конкретного інструмента.

З огляду на широке різноманіття доступних платформ, даний підпункт має

на меті провести системний аналіз найбільш поширених DLP-рішень, порівняти їх за ключовими критеріями, виявити сильні та слабкі сторони, а також оцінити доцільність використання у різних типах організацій. Такий огляд дозволить визначити, які системи є оптимальними з погляду функціональності, економічної ефективності, простоти інтеграції та відповідності сучасним вимогам до захисту інформації.

Комплексність сучасних цифрових інфраструктур зумовлює потребу оцінювати рішення для запобігання витоку даних не лише в межах однієї технології, наприклад DLP, а в контексті всієї екосистеми засобів захисту інформації. Поряд із класичними системами Data Loss Prevention сьогодні активно використовуються Cloud Access Security Brokers (CASB), платформи Data Security Posture Management (DSPM), системи управління цифровими правами (IRM/DRM), рішення класу SASE/SSE, засоби моніторингу активності баз даних (DAM), поведінкової аналітики (UEBA), шифрування та токенизації, секрет-менеджмент, а також SIEM/SOAR-платформи. Оцінювання цих рішень вимагає цілісного підходу, що враховує їхню здатність запобігати витоку даних, інтегруватися між собою, масштабуватися та відповідати нормативним вимогам.

Одним із базових критеріїв є глибина видимості даних. Це стосується того, наскільки повно система охоплює різні джерела: локальні сховища, файли на кінцевих точках, корпоративні мережі, хмарні сервіси, SaaS-платформи, сховища в контейнеризованих середовищах, DevOps-інфраструктуру та API. Рішення, які мають обмежену видимість (наприклад, не аналізують хмарні робочі області або не отримують метадані з баз даних), не можуть забезпечити ефективний захист у середовищах, де дані розподілені між десятками сервісів.

Другим критерієм виступає якість аналізу контенту та контексту. Для рішень класу DLP ключовим є контентний аналіз, тоді як для DSPM вирішальним є пошук конфіденційних даних у хмарній інфраструктурі, а для CASB — коректна інтерпретація дій у SaaS-середовищах. Оцінювання має включати здатність системи виявляти чутливу інформацію у складних сценаріях: текст у зображеннях, зашифрованих вкладеннях, вкладених архівах, потокових даних,

логах API або у структурованих таблицях. Сучасні платформи дедалі частіше використовують машинне навчання та семантичні моделі для визначення чутливості інформації, зменшення хибнопозитивних спрацьовувань та коректного аналізу складних корпоративних документів.

Не менш важливим є охоплення каналів передачі даних. У сучасних середовищах витoki можуть відбуватися не тільки через класичні мережеві протоколи або електронну пошту, але й через API-взаємодії, інтеграції DevOps, хмарні функції, тонкі клієнти, мобільні застосунки, неконтрольовані SaaS-інструменти та службові облікові записи. Системи, здатні контролювати лише традиційні канали, не можуть ефективно працювати у мультихмарних або гібридних середовищах.

Значну роль відіграє підтримка адаптивних політик безпеки. Важливо, щоб система враховувала контекст дій: геолокацію, час, роль користувача, тип пристрою, рівень ризику облікового запису, наявність підозрілих аномалій. Це дозволяє реалізовувати підхід Zero Trust і обмежувати потенційно небезпечні операції навіть у випадках, коли формально вони дозволені політиками доступу.

Окремим критерієм є масштабованість і архітектура. Корпоративні рішення повинні підтримувати розподілені розгортання, роботу в мультихмарних середовищах, масштабування під навантаженням, резервування та автоматичне балансування. Платформи, орієнтовані на середній бізнес, можуть робити акцент на простоті впровадження, тоді як крупні організації вимагають побудови багаторівневих інфраструктур з високою відмовостійкістю.

Інтеграція з існуючими системами безпеки — ще один критично важливий показник. У великих компаніях рішення мають взаємодіяти з SIEM, SOAR, IAM, PAM, NAC, CMDB, системами шифрування, DevOps-платформами та внутрішніми каталогами. Чим ширшими є інтеграційні можливості, тим ефективніше можна автоматизувати реагування й мінімізувати людський фактор.

Практична ефективність рішень оцінюється через кількість хибнопозитивних і хибнонегативних спрацьовувань, стабільність агентів, вплив на продуктивність систем, швидкість оновлення сигнатур і правил, а також якість

технічної підтримки. В оглядах великих компаній та на професійних форумах зазначається, що саме ці фактори визначають реальну експлуатаційну вартість рішень: деякі продукти можуть мати широкі функції, але при цьому генерувати надмірну кількість помилкових інцидентів або вимагати значних ресурсів адміністрування.

Ще одним вагомим аспектом є відповідність нормативним вимогам. Рішення повинні забезпечувати можливість дотримання GDPR, HIPAA, SOX, FERPA, NIS2, PCI DSS та інших регуляторів; підтримувати аудит, журналювання, інцидент-репорти, збереження лога активності, моделі контролю доступу, доказову базу для розслідувань та готовність до зовнішніх перевірок. Важливою є також підтримка корпоративних та галузевих стандартів: ISO/IEC 27001, ISO 27701, SOC 2 Type II, FedRAMP тощо.

Економічна складова відіграє не менш важливу роль. Сюди належать структура ліцензування, модель оплати (користувач, пристрій, обсяг трафіку, кількість інтеграцій), вартість підтримки, вимоги до інфраструктури, потреба у зовнішніх спеціалістах, витрати на супровід та оновлення. На практиці загальна вартість володіння (TCO) стає одним із ключових критеріїв для вибору між різними інструментами, особливо коли йдеться про масштабування.

Важливим критерієм, який виділяється в сучасних дослідженнях, є наявність поведінкової аналітики (UEBA). Платформи, здатні аналізувати профілі користувачів, виявляти аномалії та корелювати дії між різними системами, значно підвищують здатність організації запобігати інсайдерським загрозам та складним сценаріям ексфільтрації.

Оцінювання рішень також включає якість інтерфейсу та простоту управління. У великих компаніях важливі можливості автоматизації, моделювання політик, групового редагування правил, створення шаблонів, а також наочність інцидентів і звітності. У малому та середньому бізнесі акцент робиться на швидкості впровадження та мінімальній потребі у висококваліфікованому персоналі.

Таким чином, критерії оцінювання рішень для запобігання витоку даних

охоплюють широкий спектр технічних, організаційних, нормативних і експлуатаційних аспектів. Вони дозволяють порівнювати між собою не лише DLP-платформи, а й CASB, DSPM, IRM, DAM, UEBA та інші інструменти, що формують сучасну багаторівневу архітектуру захисту даних. Використання комплексної системи критеріїв створює основу для подальшого ґрунтовного аналізу ринку та дозволяє обирати рішення, які найкраще відповідають вимогам конкретної організації та її інформаційного середовища.

Оскільки витoki даних можуть виникати на різних рівнях інформаційної інфраструктури, сучасний ринок пропонує широкий спектр технологій, кожна з яких охоплює окремі аспекти безпеки. Аналіз існуючих рішень передбачає розгляд не лише класичних DLP-платформ, але й суміжних технологій, що забезпечують захист у хмарі, контролюють доступи, аналізують поведінку користувачів, захищають бази даних або керують цифровими правами. Важливою рисою сучасного підходу є те, що жоден окремий клас систем не може повністю вирішити проблему запобігання витoku, і саме тому їхні можливості доцільно розглядати у взаємодії. Порівняльний аналіз дозволяє зрозуміти, які завдання найкраще вирішує кожна технологічна група, які мають обмеження, а які здатні забезпечити комплексний захист у поєднанні одна з одною.

Традиційні системи Data Loss Prevention залишаються базовим рішенням, орієнтованим на контроль вмісту та контексту операцій з даними. Їхньою сильнішою стороною є глибокий аналіз контенту, можливість виявляти конфіденційні дані у файлах, мережевому трафіку та на кінцевих точках, а також блокування їхнього неконтрольованого передавання. У цьому аспекті DLP унікальні, оскільки жоден інший клас систем не надає настільки детального аналізу вмісту. Проте основним обмеженням традиційних DLP-платформ довгий час була недостатня видимість у хмарних середовищах та SaaS-додатках. Цей недолік частково компенсують Cloud DLP або інтеграція DLP з CASB, однак у розподілених цифрових середовищах DLP все ще потребують доповнення іншими технологіями.

CASB-платформи мають суттєві переваги там, де DLP обмежені, — у

контролі доступу до хмарних сервісів і аналізі потоків даних у SaaS-додатках. CASB надають організації повний огляд того, які хмарні ресурси використовуються, які дані передаються до зовнішніх сервісів, як користувачі взаємодіють з хмарними документами, та які сторонні додатки отримують доступ до корпоративної інформації. На відміну від DLP, ці рішення детально аналізують API-взаємодії, хмарні журнали подій та операції всередині багаторівневих SaaS-середовищ. Завдяки цьому CASB стають незамінними для організацій, де велика частина даних обробляється у хмарі. Однак CASB не можуть замінити DLP у контентному аналізі, оскільки їхні можливості щодо глибокої інспекції файлів є обмеженими.

Окремий інтерес викликають системи Data Security Posture Management — DSPM, які з'явилися відносно недавно, але швидко стали одним із ключових елементів хмарної безпеки. На відміну від DLP і CASB, DSPM не займаються блокуванням передачі даних, а фокусуються на виявленні того, де зберігаються конфіденційні дані, хто має до них доступ і чи відповідають налаштування хмарних ресурсів політикам безпеки. У складних хмарних архітектурах DSPM може виявити сотні помилкових дозволів, публічних S3-бакетів, неправильно сконфігурованих баз даних або надмірних API-ключів. Цей клас рішень не конкурує з DLP, а доповнює його, надаючи «картину зверху» та дозволяючи автоматично виправляти конфігураційні недоліки. Проте DSPM не забезпечує контроль каналів передачі даних, тому не може працювати самостійно як система запобігання витоку.

Суттєво відрізняється функціональність систем Information Rights Management і Digital Rights Management, які захищають документи шляхом накладання на них криптографічних і політичних обмежень. На відміну від DLP, які контролюють передачу даних, IRM/DRM супроводжує документ навіть за межами організації. Це означає, що користувач, отримавши файл, може читати його лише в дозволених умовах, а спроби копіювання, друку, скриншотів або експорту можуть бути фізично заборонені. Порівняно з DLP, ці рішення мають значно глибший контроль над доступом до вже переданих даних, але вони не

забезпечують виявлення або блокування каналів витоку, фактично починаючи діяти лише після передачі файлу. Тому вони ефективні в умовах співпраці з партнерами та зовнішніми контрагентами, але не вирішують весь спектр загроз самостійно.

Не менш важливою групою є рішення класу UEBA — User and Entity Behavior Analytics. Вони працюють на рівні поведінкових профілів і дозволяють виявляти інциденти, які традиційні системи не фіксують. Збільшення швидкості роботи з файлами, раптове завантаження масиву документів, доступ до нетипових систем або експорт даних у незвичний час можуть сигналізувати про інсайдерську активність або компрометацію облікового запису. UEBA не блокують витoki напpямy, але стають критичним елементом у виявленні складних ланцюгів атак, які обходять класичні захисні інструменти. Їхня цінність особливо проявляється при поєднанні з DLP, CASB або SIEM, де поведінкова аналітика надає необхідний контекст для прийняття рішень щодо блокування.

Для середовищ, де основним об'єктом захисту є бази даних, ключовими стають системи Database Activity Monitoring. DAM контролюють усі запити до корпоративних БД, аналізують їхню аномальність, виявляють спроби копіювання великих масивів даних, SQL-експортів або несанкціонованих операцій зі службових облікових записів. На відміну від DLP, які фокусуються на файлах і каналах передачі, DAM захищають саму основу корпоративної інформаційної інфраструктури — дані у стані зберігання. Проте ці системи не контролюють дії після того, як інформацію вже вилучено з бази, що робить їх ефективними лише на одному етапі життєвого циклу даних.

Важливу роль у сучасних архітектурах відіграють SIEM- та SOAR-рішення. Вони не запобігають витокам напpямy, але координують роботу всіх інших систем. SIEM збирає, корелює та аналізує події з DLP, DSPM, CASB, UEBA та інших інструментів, формуючи цілісну картину інцидентів. SOAR автоматизує реагування: блокує обліковий запис, ізолює пристрій, скасовує ключ доступу, активує форензичний збір даних. У складних середовищах саме SIEM+SOAR визначають, чи зможе організація оперативно зупинити інцидент, виявлений DLP

або іншою системою.

На окрему увагу заслуговують рішення шифрування та токенизації. Хоча вони не блокують витоки, їхня роль критична у зниженні впливу інцидентів. Зашифровані дані, навіть якщо вони були ексфільтровані, залишаються непридатними без ключів. Це робить такі технології важливим доповненням DLP або DAM. Проте шифрування не здатне запобігти витoku легально доступних даних — співробітник, що має ключ, може передати файл у розшифрованому вигляді. Саме тому шифрування завжди застосовується у складі багаторівневої стратегії.

Порівняння цих груп рішень демонструє, що жодна з них не забезпечує універсального захисту. DLP контролює рух даних, CASB — хмарні потоки, DSPM — конфігурацію сховищ, IRM — життєвий цикл документів за межами організації, DAM — доступ до баз даних, UEBA — поведінку користувачів, SIEM/SOAR — координацію інцидентів. Їхні функції не дублюють одна одну, а формують багаторівневу архітектуру, здатну протистояти як випадковим, так і навмисним витокам.

У контексті сучасних інфраструктур найбільш ефективними виявляються комбіновані моделі, де DLP взаємодіє з CASB для контролю хмарних потоків, DSPM забезпечує аудит конфігурацій, DAM — контроль доступу до структурованих даних, а UEBA додає поведінковий аналіз. Саме така інтегрована модель відповідає принципам Zero Trust та Data-Centric Security й дозволяє організаціям істотно знизити ризик витоку інформації у складних і розподілених цифрових екосистемах.

Світовий ринок технологій запобігання витоку даних представлений широким спектром корпоративних рішень, які відрізняються рівнем інтеграції, функціональністю, архітектурою та підходами до реалізації контролю даних. Класичні DLP-платформи займають центральне місце у цій екосистемі, адже забезпечують глибокий контентно-контекстний аналіз, інспекцію всіх ключових каналів передавання інформації та моніторинг дій користувачів. Проте навіть серед рішень цього класу існують суттєві відмінності, що визначають їхню

ефективність у конкретних цифрових середовищах. Аналіз провідних світових продуктів дозволяє сформулювати об'єктивне уявлення про можливості сучасних DLP та їхню роль у комплексній архітектурі безпеки.

Одним із найвідоміших та найпоширеніших рішень є Symantec (Broadcom) Data Loss Prevention, яке вже понад десять років залишається одним із лідерів ринку у звітах Gartner та Forrester. Система вирізняється високою глибиною контентного аналізу, розвиненими методами визначення чутливих даних і великим набором попередньо створених політик відповідності. Архітектура Symantec базується на централізованому сервері, агентній взаємодії з кінцевими точками та мережевими моніторами, здатних аналізувати трафік у режимі близькому до реального часу. Потужною стороною Symantec є можливість виявляти складні структури даних, зокрема комбінації полів або вкладених об'єктів, що робить систему придатною для великих фінансових, телекомунікаційних і державних організацій. Проте її складність впровадження, висока ресурсомісткість і значні витрати на підтримку часто роблять продукт менш привабливим для середнього бізнесу. Деякі клієнти відзначали на форумах, що налаштування агентів та оновлення політик потребують значного часу, а інтеграція з хмарними сервісами вимагає додаткових модулів, що підвищує загальну вартість володіння.

Суттєву конкуренцію Symantec становить Forcepoint DLP — система, що поєднує класичний контентний аналіз із поведінковими моделями. Особливість цього продукту полягає в тому, що він інтегрований із власною платформою UEBA, яка враховує ризик-профілі користувачів і може адаптувати політики залежно від поведінки. Це дозволяє Forcepoint визначати потенційно небезпечні дії ще до того, як користувач завершить операцію з даними, наприклад, при спробі нестандартного копіювання файлів або виконання масових операцій зі службовими документами. Система має розвинену архітектуру контролю кінцевих точок, включно з управлінням пристроями, виявленням скріншотів і блокуванням клауд-операцій у режимі реального часу. На практиці Forcepoint часто обирають компанії, що прагнуть поєднати DLP та аналіз поведінки у єдиному рішенні, але користувачі на Reddit і Spiceworks відзначають, що

інтерфейс керування є менш інтуїтивним, ніж у конкурентів, а продуктивність агентів може впливати на роботу слабших систем.

Ще одним великим гравцем на ринку є McAfee DLP (нині Trellix), яке давно застосовується у великих організаціях завдяки своїй масштабованості та можливості одночасно керувати численними кінцевими точками. Напрямок, у якому McAfee вирізняється, є інтеграція з іншими рішеннями компанії — антивірусами, EDR/XDR, SIEM та системами управління ідентичностями. Такий комплекс дозволяє створити єдину платформу безпеки, де DLP є складовою частиною ширшої екосистеми. Проте за останні роки користувачі відзначали, що продукт оновлюється повільніше, ніж рішення конкурентів, а його інструменти класифікації не такі гнучкі, як у Microsoft Purview або Forcepoint. Попри це McAfee залишається поширеним вибором у фінансовому секторі, де важлива централізована політика безпеки.

На тлі класичних розгорнутих DLP-рішень особливе місце посідає Microsoft Purview DLP — платформа, що інтегрована у Microsoft 365 і працює без додаткової інфраструктури. Її головна перевага полягає в глибокій інтеграції з хмарними сервісами Microsoft, включно з Exchange, Teams, SharePoint, OneDrive та Windows 11. Purview надає широкий набір шаблонів для відповідності вимогам GDPR, HIPAA, PCI DSS та інших регуляторів, а також пропонує автоматичну класифікацію на основі машинного навчання. У корпоративних середовищах Microsoft DLP показує високу ефективність саме через природну інтеграцію в робочі процеси користувачів та автоматизовану видимість у хмарних операціях. Обмеженням Purview є його слабша робота з не-Microsoft системами: для повноцінного контролю сторонніх сервісів потрібен CASB Microsoft Defender for Cloud Apps. Однак за рахунок зручності адміністрування, інтуїтивного інтерфейсу та низької вартості володіння платформа стає одним з найпопулярніших рішень серед бізнесів, що активно використовують хмарні сервіси Microsoft.

Варто згадати й Digital Guardian — одне з небагатьох DLP-рішень, що пропонує контроль на рівні ядра операційної системи. Завдяки цьому продукт забезпечує унікальні можливості моніторингу, зокрема виявлення операцій, які

інші системи не можуть відстежити. Digital Guardian традиційно використовують компанії з високими вимогами до захисту інтелектуальної власності — фармацевтичні корпорації, оборонні підприємства, інженерні центри та наукові установи. Система демонструє високу ефективність у контролі складних форматів САД-файлів, технічної документації та вихідного коду. Обмеженням є висока складність адміністрування та високі апаратні вимоги, що робить продукт менш зручним для середніх компаній.

До найбільш технологічно розвинених можна віднести рішення GTB Technologies. На відміну від багатьох конкурентів, GTB використовує власний механізм контентної індексації, який дозволяє системі виявляти конфіденційні блоки інформації навіть у сильно модифікованих або частково змінених документах. Це корисно у випадках, коли співробітники намагаються обійти політики, фрагментуючи або переформатовуючи чутливі дані. GTB також підтримує двосторонній контроль хмарних сервісів і надає детальний моніторинг API-взаємодій. У відгуках зазначають, що сильна сторона GTB — точність визначення контенту, тоді як мінусами є складність конфігурування та обмежений вибір інтеграцій.

Cisco Secure DLP (раніше Cisco Cloudlock) більше орієнтоване на хмарні середовища та SaaS — система дозволяє контролювати операції у Google Workspace, Salesforce, Slack, Box та інших сервісах. Хоча за глибиною контентного аналізу Cisco поступається класичним DLP-рішенням, його перевагою є ефективність у великих хмарних екосистемах, де ключову роль відіграє видимість у взаємодії користувачів з онлайн-ресурсами. Cisco також пропонує інтеграцію з Meraki та іншими мережевими продуктами компанії, що дозволяє будувати захист на рівні інфраструктури. Проте система менш придатна для організацій, що потребують детального аналізу локальних операцій з файлами.

Порівняння цих рішень демонструє, що ринок DLP не є однорідним і кожна платформа орієнтована на власну групу сценаріїв. Symantec і Forcepoint підходять для великих підприємств з високими вимогами до точності аналізу та глибини

контролю. Microsoft Purview найкраще інтегрується у хмарні середовища Microsoft, McAfee/Trellix орієнтований на комплексність екосистеми безпеки, а Digital Guardian та GTB — на захист специфічних типів даних та великих обсягів технічної інформації. Цей різноманітний ландшафт вказує на те, що вибір DLP-рішення повинен базуватися не на рейтингах, а на реальних бізнес-процесах, структурі даних та потребах організації.

Серед технологій, що доповнюють DLP у комплексній архітектурі безпеки, особливо важливими є рішення класу CASB, DSPM, UEBA і DAM. Вони формують додаткові рівні контролю, необхідні в умовах, коли корпоративні дані виходять за межі традиційних периметрів, переміщуються між хмарними сервісами, SaaS-додатками, мобільними платформами, мікросервісною архітектурою й різноманітними інтеграційними точками. Оскільки сучасні організації все частіше використовують хмарні інструменти для зберігання, обробки та спільної роботи з інформацією, класичні DLP-рішення не завжди забезпечують необхідний рівень видимості. Саме тому в екосистемі захисту виникли інструменти, що зосереджуються на контролі API-взаємодій, аудиті конфігурацій, аналізі поведінки користувачів та моніторингу структурованих даних, а їхнє поєднання з DLP значно підсилює загальну стратегію превенції витоків.

Однією з ключових груп технологій є Cloud Access Security Broker — CASB. Ці системи стали відповіддю на масштабне впровадження хмарних сервісів, таких як Microsoft 365, Google Workspace, Salesforce, ServiceNow, Workday та сотні інших SaaS-рішень, які стали критично важливими для бізнес-процесів. CASB функціонують як посередник між користувачем і хмарним сервісом та забезпечують повну видимість того, як дані переміщуються всередині хмарного середовища. На відміну від DLP, які працюють здебільшого на рівні контенту, CASB контролюють API-виклики, журнали операцій, дозволи, конфігурації та політики доступу у SaaS-платформах.

Серед найбільш розвинених рішень CASB можна виділити Microsoft Defender for Cloud Apps, Netskope, McAfee MVISION Cloud, Palo Alto Networks

Prisma Cloud, Cisco Cloudlock і Lookout CASB. Microsoft Defender for Cloud Apps вирізняється глибокою інтеграцією з Microsoft 365 і ефективністю в управлінні дозволами, токенами доступу та API-взаємодіями у хмарній екосистемі Microsoft. Netskope є одним із лідерів ринку завдяки архітектурі з «інспекцією в реальному часі», що забезпечує контроль над даними під час їхнього переміщення між SaaS-додатками. Prisma Cloud спеціалізується на багатохмарних середовищах і контейнерних інфраструктурах, забезпечуючи виявлення помилкових конфігурацій, які часто стають джерелами витоків. Cisco Cloudlock орієнтований на простоту впровадження і добре інтегрується з корпоративними мережевими рішеннями Cisco, що робить його популярним серед компаній, які використовують централізовану інфраструктуру Cisco Secure.

Важливою категорією є рішення класу DSPM — Data Security Posture Management. Технології цього класу виникли як відповідь на проблему «незримості» даних у хмарних середовищах, коли IT-відділ не може точно визначити, де саме зберігаються конфіденційні дані, хто має до них доступ і чи відповідають налаштування хмарних сховищ політикам безпеки. На практиці DSPM-рішення автоматично сканують хмарні середовища, виявляють конфіденційні дані, визначають надмірні дозволи, аналізують ризикові конфігурації та повідомляють про потенційні точки витoku. Вони не замінюють DLP, але є важливим інструментом для побудови цілісної моделі керування даними.

Серед сучасних лідерів DSPM — Wiz, BigID, Varonis, IBM Guardium Insights та Cyera. Wiz за короткий період став одним із найпопулярніших рішень у світі завдяки здатності виконувати глибокий аналіз хмарної інфраструктури, виявляти «надлишкові дозволи» (toxic combinations of permissions) та помилки конфігурації. Varonis, у свою чергу, спеціалізується на виявленні даних у структурованих і неструктурованих сховищах, аналізі ролей і політик доступу. BigID використовує алгоритми машинного навчання для автоматичного визначення конфіденційної інформації й формування профілів ризиків. DSPM-рішення особливо корисні для організацій, які мають складні хмарні інфраструктури або обробляють великі

обсяги даних у режимах багатохмарності та мультиорендності.

У контексті інсайдерських загроз важливу роль відіграють рішення класу UEBA — User and Entity Behavior Analytics. На відміну від DLP і CASB, які здебільшого працюють із контентом і дозволами, UEBA аналізує поведінку користувачів, створює статистичні моделі нормальної активності та виявляє аномалії. Загалом UEBA не запобігає витоку самостійно, але забезпечує виявлення складних сценаріїв інсайдерської активності або компрометації облікових записів, які не виявляються класичними інструментами. UEBA-рішення використовують машинне навчання, імовірнісні моделі та аналіз відхилень для формування ризикових профілів користувачів. Наприклад, якщо співробітник, який зазвичай працює з невеликим набором документів у робочий час, раптом починає масово завантажувати файли у нічний час або отримує доступ до нетипових ресурсів, система позначає таку активність як аномальну.

До найпопулярніших UEBA-рішень належать Splunk User Behavior Analytics, Exabeam, Securonix, Varonis UBA та Microsoft Defender for Identity. Splunk UBA вважається одним із найточніших завдяки своїй моделі кореляції подій та масштабованій аналітичній платформі. Exabeam вирізняється можливістю автоматично реконструювати ланцюжки атак та формувати повну історію дій користувачів. Securonix пропонує глибоке поведенкове моделювання та активно застосовується у великих фінансових установах. UEBA-технології особливо ефективні, коли поєднуються з DLP або SIEM, адже поведінковий контекст дозволяє відрізнити шкідливу спробу ексфільтрації від легітимної операції.

Системи DAM — Database Activity Monitoring — є критично важливим елементом архітектури захисту від витоку для організацій, які використовують великі бази даних. Ці рішення контролюють усі запити до БД у режимі близькому до реального часу, аналізують операції читання, зміни, експорту та масових вибірок, виявляють аномалії та порушення політик доступу. DAM не конкурують з DLP, а захищають дані на найнижчому рівні — у момент, коли вони знаходяться у структурованому середовищі. Якщо DLP контролює канали передавання

інформації, то DAM контролює джерело, забезпечуючи моніторинг доступу до таблиць, полів, транзакцій або службових облікових записів. Одним з ключових сценаріїв застосування DAM є виявлення масових SQL-експортів або спроби читання конфіденційних полів співробітниками, які не мають відповідних повноважень.

Найбільш відомими DAM-рішеннями є IBM Guardium, Imperva SecureSphere, Oracle Audit Vault and Database Firewall, McAfee Database Security та Datadog Cloud SIEM (з модулем Database Monitoring). IBM Guardium має потужні можливості аудиту, ізоляції транзакцій та контролю конфіденційних наборів даних. Imperva SecureSphere забезпечує глибоку інспекцію SQL-трафіку та здатна блокувати запити в режимі реального часу. Oracle AVDF краще інтегрується з Oracle Database та ефективний у великих корпоративних середовищах. Усі ці рішення дозволяють запобігати витоку безпосередньо на рівні систем управління базами даних, що є критичним для банків, медичних організацій та державних структур.

Порівняння CASB, DSPM, UEBA та DAM демонструє, що хоча ці рішення не конкурують із DLP, вони значно розширюють можливості організації щодо запобігання витоку даних. CASB забезпечує контроль над хмарними потоками, DSPM — над конфігураціями та розташуванням даних, UEBA — над поведінкою користувачів, DAM — над доступом до структурованої інформації. Саме поєднання цих технологій зі звичайним DLP створює багаторівневу оборону, яка відповідає сучасним принципам Zero Trust та Data-Centric Security.

У сучасній архітектурі безпеки, орієнтованій на дані (Data-Centric Security), критично важливою є здатність не лише контролювати переміщення інформації, але й зберігати її захищеною незалежно від місця розташування, формату зберігання чи каналу передачі. У цьому контексті вагому роль відіграють технології IRM/DRM, криптографічні рішення (шифрування й токенизація), а також системи управління журналами та інцидентами безпеки — SIEM і SOAR. У комплексі з DLP та іншими інструментами вони формують повноцінну модель захисту, що дає змогу створювати багаторівневі бар'єри на шляху ексфільтрації

інформації й оперативно реагувати на інциденти. Саме ці технологічні класи закривають так звану «зону після витоку», тобто гарантують, що навіть якщо дані опинилися у неналежних руках, вони не будуть використані або розкриті.

Однією з ключових груп рішень, що забезпечують захист даних у динамічному середовищі, є IRM (Information Rights Management) та DRM (Digital Rights Management). IRM/DRM-контроль базується на впровадженні обмежень на рівні самих документів — вони «несуть» у собі політику доступу незалежно від того, куди потрапляють: у локальні сховища, хмарні сервіси, листи електронної пошти або сторонні організації. У контексті запобігання витоку це означає, що навіть якщо файл був скопійований, пересланий або завантажений за межі корпоративного периметра, система зберігає контроль над його відкриттям, друком, копіюванням, експортом, зняттям скриншотів чи передаванням через сторонні канали.

Найбільш відомими IRM/DRM-рішеннями є Microsoft Azure Information Protection (AIP), Microsoft Purview Information Protection, Seclore, Vera (раніше — VeraSecurity), Adobe Experience Manager DRM та Fasoo Enterprise DRM. Microsoft AIP широко використовується у великих організаціях через інтеграцію з Microsoft 365 і можливість автоматичного застосування політик до документів на основі класифікації. Seclore вирізняється детальним контролем за користувацькими діями, включно зі спробами друку, копіювання або роботи в автономному режимі. Fasoo користується популярністю в банківському секторі, де необхідні суворі обмеження щодо розповсюдження документів.

Для великих організацій IRM/DRM є важливим інструментом не лише запобігання витокам, але й забезпечення регуляторної відповідності. Наприклад, відповідно до GDPR компанії зобов'язані вживати заходів, що гарантують обмеження доступу до персональних даних і запобігання їхньому несанкціонованому розголошенню. IRM дозволяє реалізувати це на документальному рівні: файл, що містить персональні дані, може бути відкритий лише на авторизованих пристроях і лише тими користувачами, які отримали відповідні права.

Другим важливим напрямом є криптографічний захист інформації — шифрування та токенизація. Шифрування є фундаментальним інструментом запобігання витокам, оскільки унеможливорює використання інформації у разі її ексфільтрації, якщо відсутній ключ дешифрування. Токенизація, своєю чергою, замінює реальні дані умовними маркерами (токенами) так, що навіть у випадку компрометації зловмисники отримують непридатні до використання набори.

Серед найбільш застосовуваних рішень можна виокремити Thales CipherTrust, Symantec Encryption, IBM Guardium Encryption, Protegrity Tokenization Platform та AWS KMS (Key Management Service). Thales є одним із лідерів ринку завдяки можливості централізованого управління ключами та застосування шифрування на різних рівнях: файлів, баз даних, контейнерів та хмарних сховищ. Protegrity спеціалізується на токенизації та широко використовується у фінансових установах, які мають дотримуватися PCI DSS. AWS KMS, інтегрований у хмарну екосистему Amazon, забезпечує гнучке управління ключами та застосовується у багатьох компаніях, що працюють у моделі хмарної інфраструктури.

Важливість криптографічного захисту суттєво зросла у зв'язку з тим, що дедалі більше організацій працюють із розподіленими системами, мікросервісами, контейнерами та хмарними платформами. Шифрування дає змогу забезпечити контроль над інформацією незалежно від того, чи передається вона між сервісами, чи зберігається в базах даних, чи імпортується сторонніми системами. Підхід «шифрування за замовчуванням» (Encryption by Default) дедалі частіше стає регуляторною вимогою: він передбачає, що всі критичні набори даних мають бути зашифрованими у стані спокою (at rest) і під час передачі (in transit).

Тісно пов'язаними з криптографічними методами є системи SIEM — Security Information and Event Management. SIEM-рішення забезпечують збір, агрегування, кореляцію та аналіз журналів подій з усіх систем безпеки — DLP, CASB, UEBA, мережевого обладнання, кінцевих точок, хмарних платформ, серверів і баз даних. У контексті запобігання витоку SIEM дозволяє:

- виявляти складні ланцюжки атак, що включають підготовчі дії перед ексфільтрацією;

- аналізувати аномалії, які не є очевидними на рівні окремих систем;
- корелювати поведінку користувачів і технічні події з ризиковими сценаріями;
- формувати хронологію інцидентів та забезпечувати доказову базу.

До найпотужніших SIEM-платформ належать Splunk Enterprise Security, IBM QRadar, Microsoft Sentinel, Elastic Security, Exabeam Fusion SIEM, LogRhythm XDR Stack та ArcSight. Splunk широко застосовується у великих корпораціях завдяки своїм можливостям розподіленої обробки логів і побудови складних кореляційних правил. IBM QRadar відомий своєю точністю у виявленні аномалій і можливістю аналізувати великі обсяги даних без значних втрат продуктивності. Microsoft Sentinel вирізняється глибокою інтеграцією з Azure і Microsoft 365, що забезпечує ефективну видимість у хмарних середовищах.

Системи SIEM відіграють важливу роль не лише у виявленні фактів ексфільтрації, але й у формуванні моделей загроз. Вони дозволяють визначити тенденції, аналізувати поведінку окремих груп користувачів, виявляти нетипові запити до баз даних, спроби обходу політик DLP або взаємодії з підозрілими ресурсами. Саме завдяки кореляційним механізмам SIEM здатен об'єднати дані з DLP, UEBA, DAM і CASB та формувати цілісну картину інциденту.

У більшості сучасних архітектур SIEM працює в тандемі з SOAR — Security Orchestration, Automation and Response. SOAR-системи забезпечують автоматизацію процесів реагування на інциденти, що значно зменшує час між виявленням загрози та вжиттям заходів. В умовах витоку даних це означає, що система може:

- автоматично заблокувати акаунт, який демонструє підозрілу поведінку;
- ізолювати робочу станцію;
- заблокувати мережеве з'єднання або API-сесії;
- повідомити відповідальних осіб;
- зібрати форензичні артефакти;
- оновити політику доступу або DLP-правило в реальному часі.

Найпоширенішими SOAR-рішеннями є Palo Alto Networks Cortex XSOAR, Splunk SOAR (раніше Phantom), IBM Resilient, DFLabs IncMan SOAR, Siemplify

(тепер частина Google Cloud) та Rapid7 InsightConnect. Cortex XSOAR надає широкий набір інтеграційних модулів і дозволяє автоматизувати складні сценарії реагування. Splunk SOAR відомий гнучкістю та можливістю створення візуальних плейбуків. IBM Resilient часто використовується у фінансовому секторі, де потрібні детальні регламенти реагування.

Поєднання SIEM і SOAR стає особливо ефективним у випадках, коли виявлення витоку відбувається в режимі реального часу. Наприклад, якщо DLP фіксує спробу ексфільтрації великого обсягу даних, SIEM корелює цю подію з попередніми діями користувача, а SOAR автоматично блокує доступ і запускає розслідування. Такий триєдиний механізм дає змогу зупиняти витoki ще на етапі ініціації.

Узагальнюючи, рішення IRM/DRM, криптографічні інструменти, SIEM і SOAR відіграють критичну роль у багатошаровому захисті даних. Якщо DLP забезпечує контроль над каналами й контентом, CASB — над хмарними потоками, DSPM — над конфігураціями, UEBA — над поведінкою користувачів, DAM — над доступом до баз даних, то IRM/DRM і криптографія гарантують, що навіть у разі витоку дані залишаються недоступними, а SIEM/SOAR забезпечують оперативне виявлення й реагування.

У сучасній архітектурі захисту даних важливе місце посідають не лише класичні DLP-, CASB-, DSPM-, UEBA- та DAM-рішення, але й додаткові технологічні класи, які створюють додаткові бар'єри на шляху витоку інформації. До таких належать системи контролю доступу до мережі (NAC), платформи класу EDR/XDR, рішення керування мобільними пристроями та застосунками (MDM/MAM), інструменти DevSecOps, а також платформи Data Governance, що забезпечують цілісне управління життєвим циклом даних. Разом вони формують багатошарову екосистему, в якій запобігання витоку стає не точковою функцією окремого продукту, а властивістю всієї цифрової інфраструктури.

Системи Network Access Control (NAC) історично з'явилися як інструмент, що дозволяє контролювати допуск пристроїв до корпоративної мережі, виходячи з їхнього стану безпеки. У контексті запобігання витокам даних NAC відіграє роль

«воріт» для кінцевих точок: лише ті пристрої, які відповідають політикам (наявність антивірусу, шифрування дисків, актуальні патчі, активний агент безпеки), отримують доступ до внутрішніх ресурсів. Завдяки цьому знижується ймовірність того, що неавторизовані або скомпрометовані пристрої будуть використовуватися як канал ексфільтрації. Рішення Cisco Identity Services Engine (ISE), Aruba ClearPass, Forescout та інші провідні NAC-платформи дозволяють сегментувати мережу, розділяти доступ для гостей, підрядників, IoT-пристроїв і співробітників, а також динамічно змінювати політики залежно від ризику, виявленого за допомогою DLP, UEBA чи EDR. Наприклад, у випадку фіксації підозрілих дій на робочій станції система може автоматично перевести її у карантинний сегмент, де доступ до критичних ресурсів обмежений, що унеможливорює масовий витік інформації.

Платформи класу EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response) фокусуються на виявленні, аналізі та нейтралізації загроз на рівні кінцевих точок і розширеної інфраструктури (сервери, хмара, мережа). Хоча їхня першочергова мета — боротьба зі шкідливим ПЗ, експлойтами та складними атаками, вони мають прямий зв'язок із запобіганням витоку даних. EDR-системи реєструють будь-які аномальні дії на рівні процесів, файлів, мережевих з'єднань і можуть виявляти сценарії, коли зловмисник або інсайдер готує ексфільтрацію: масове архівування документів, запуск власних скриптів для копіювання вмісту каталогів, підключення до нетипових зовнішніх ресурсів. XDR-платформи, поєднуючи дані з кінцевих точок, мережі, хмари й поштових систем, дозволяють побачити повний ланцюг атаки: від фішингового листа до спроби вивантаження масиву даних на зовнішній сервер. Рішення таких вендорів, як CrowdStrike, Microsoft Defender for Endpoint, Palo Alto Cortex XDR, SentinelOne, Trend Micro та інші, дедалі частіше інтегруються з DLP- та SIEM-платформами. Це дає змогу автоматично блокувати процеси, що використовуються для ексфільтрації, або обмежувати права користувача, якщо виявлено, що його обліковий запис бере участь у потенційно шкідливих діях.

Важливою складовою запобігання витоку є також керування мобільними

пристроями та застосунками, що реалізується через MDM (Mobile Device Management) та MAM (Mobile Application Management). Оскільки значна частина роботи виконується на смартфонах, планшетах і ноутбуках, нерідко у змішаних BYOD-сценаріях (коли співробітники використовують власні пристрої), ці канали стають високоризиковими з погляду витоку. MDM-системи дозволяють забезпечити шифрування мобільних пристроїв, примусовий PIN-код або біометрію, контроль встановлених застосунків, можливість дистанційного очищення даних. MAM зосереджується на керуванні корпоративними застосунками й контейнерами, відокремлюючи робочі дані від особистих. Рішення Microsoft Intune, VMware Workspace ONE, MobileIron (нині Ivanti), Citrix Endpoint Management та інші підтримують інтеграцію з DLP-політиками, дозволяючи блокувати копіювання інформації з корпоративних застосунків у неавторизовані програми чи особисті сховища. Таким чином, навіть якщо співробітник працює з чутливими даними зі смартфона, організація зберігає контроль над тим, куди ці дані можуть бути експортовані, а куди — ні.

Окремий напрям пов'язаний з інтеграцією безпеки в процеси розробки — так званий DevSecOps. З погляду запобігання витоку даних DevSecOps важливий тим, що дозволяє уникати появи критичних конфігураційних помилок і «секретів у коді», які можуть стати джерелом ексфільтрації. Інструменти статичного (SAST) та динамічного (DAST) аналізу коду, сканери секретів (наприклад, GitGuardian, TruffleHog, Gitleaks), аналіз безпеки контейнерів і pipeline-сканери перевіряють, чи не містить вихідний код або конфігураційні файли паролів, ключів доступу до баз даних, токенів API або відладкових дамів із реальними даними. У разі виявлення таких артефактів система блокує злиття змін до основної гілки або автоматично відкликає ключі. Це дозволяє запобігти ситуаціям, коли конфіденційні дані випадково потрапляють до публічних репозиторіїв або тестові середовища, відкриті в Інтернеті.

Платформи Data Governance відіграють роль «керуючого центру» для всіх процесів, пов'язаних із даними. Якщо DLP, CASB, DSPM, DAM, SIEM і інші інструменти відповідають за технічний контроль, то Data Governance визначає

політики, правила, відповідальних осіб, процеси й регламенти, за якими ці інструменти мають працювати. Сучасні платформи управління даними, такі як Collibra, Informatica Axon, OneTrust Data Governance, SAP Information Steward та інші, забезпечують каталогізацію даних, опис бізнес-термінів, визначення власників наборів даних (data owners), побудову схем походження інформації (data lineage) та оцінку ризиків. У контексті запобігання витоку саме Data Governance дає відповідь на питання: які дані вважаються критичними, де вони знаходяться, хто за них відповідає, які політики мають бути застосовані та як контролюється їхнє виконання. Наприклад, якщо в системі Data Governance визначено, що певний набір даних містить персональну медичну інформацію, до нього автоматично мають застосовуватися посилені політики DLP, шифрування та IRM, а доступ — обмежуватися конкретною групою користувачів.

Узагальнюючи, можна зазначити, що запобігання витоку даних в організації — це результат взаємодії великої кількості інструментів, а не функція одного окремого рішення. DLP-системи виконують роль ядра, яке контролює контент і контекст операцій із даними на каналах передавання та кінцевих точках. CASB забезпечує видимість і контроль хмарних сервісів і SaaS-додатків. DSPM відповідає за оглядову картину розташування та конфігурації даних у хмарі. UEBA аналізує поведінку користувачів і виявляє аномалії. DAM стежить за доступом до баз даних. NAC контролює допуск пристроїв до мережі. EDR/XDR виявляє атаки й шкідливі дії, які можуть призвести до витоку. MDM/MAM зменшують ризик витоку через мобільні й особисті пристрої. DevSecOps інструменти запобігають потраплянню чутливої інформації до коду, репозиторіїв та тестових середовищ. IRM/DRM і криптографія гарантують, що навіть у разі витоку дані залишаються непридатними для зловмисників. SIEM та SOAR забезпечують кореляцію подій та автоматизацію реагування, тоді як Data Governance формує єдину політико-процесну основу для всього цього комплексу.

Для наочності ключові групи рішень, які використовуються для запобігання витоку даних, можна звести у зведену порівняльну таблицю, що демонструє їхню основну роль, сильні сторони та обмеження з точки зору захисту даних:

Таблиця -- 1

Клас рішень	Основна мета в контексті витоків даних	Ключовісильні сторони	Основні обмеження	Типові сценарії використання
DLP	Контроль контенту та контексту операцій з даними	Глибокий аналіз вмісту, політики за типами даних, блокування каналів, журналювання	Висока складність впровадження, потреба у точному налаштуванні, можливі помилкові спрацьовування	Захист файлів і повідомлень, контроль e-mail, веб, USB, друку, кінцевих точок
CASB	Контроль доступу до хмарних сервісів і SaaS	Видимість хмарних потоків, контроль API, управління дозволами, виявлення неправильних конфігурацій	Обмежена глибина аналізу локальних операцій, залежність від підтримуваних сервісів	Безпечна робота з Microsoft 365, Google Workspace, Salesforce, Slack, іншими SaaS
DSPM	Аналіз розташування й конфігурації конфіденційних даних у хмарі	Автоматичне виявлення чутливої інформації, аналіз дозволів, оцінка ризиків	Не блокує дії напрямку, потребує інтеграції з DLP/CASB/IRM	Огляд хмарних сховищ, виявлення «зайвих» прав доступу, ризикових bucket'ів, баз даних
	Виявлення	Виявлення складних	Не запобігає витoku	Аналіз нетипових

Клас рішень	Основна мета в контексті витоків даних	Ключові/сильні сторони	Основні обмеження	Типові сценарії використання
UEBA	аномальної поведінки користувачів і сутностей	інсайдерських сценаріїв, побудова поведінкових профілів	самостійно, потребує якісних даних із інших систем	доступів, масового копіювання, нічної активності, нестандартних транзакцій
DAM	Моніторинг і контроль діяльності в базах даних	Глибокий контроль SQL-операцій, виявлення масових вибірок, аудит доступу	Зосереджений лише на рівні БД, не контролює подальший шлях даних	Захист фінансових, медичних, державних БД, аудит операцій адміністраторів
NAC	Контроль доступу пристроїв до мережі	Перевірка стану безпеки кінцевих точок, динамічна сегментація, ізоляція підозрілих вузлів	Не аналізує контент даних, потребує інтеграції з іншими системами	Обмеження доступу гостей, BYOD- та IoT-пристроїв, карантин скомпрометованих станцій
EDR/XDR	Виявлення та реагування на загрози на кінцевих точках і в інфраструктурі	Виявлення складних атак, шкідливих процесів, командно-контрольних каналів, кореляція подій	Орієнтовані на загрози, а не власне на типи даних, можуть створювати інформаційний шум	Виявлення шкідливих скриптів, ransomware, lateral movement, підготовки до ексфільтрації

Клас рішень	Основна мета в контексті витоків даних	Ключові/сильні сторони	Основні обмеження	Типові сценарії використання
MDM/MAM	Захист мобільних і BYOD-пристроїв, розділення особистих і робочих даних	Шифрування пристроїв, контроль застосунків, видалення даних, ізоляція корпоративних контейнерів	Залежність від мобільних платформ, складність у сценаріях з високою гнучкістю BYOD	Дистанційна робота, мобільний доступ до пошти, документів, CRM, корпоративних застосунків
IRM/DRM	Збереження контролю над документами поза периметром	Обмеження відкриття, друку, копіювання, шифрування вмісту, політики «вшиті» в документ	Можливі проблеми з юзабіліті, сумісністю, потреба в агентському ПЗ або підтримці на стороні клієнта	Захист документів, пересланих партнерам, постачальникам, робота з файлами поза мережею організації
Шифрування/ токенізація	Унеможливлення використання даних без ключів чи де-токенізації	Захист «у спокої» і «в польоті», відповідність вимогам регуляторів, централізоване управління ключами	Не запобігає витоку сам по собі, важливо правильне управління ключами	Захист дисків, сховищ, БД, резервних копій, платіжних і персональних даних

Клас рішень	Основна мета в контексті витоків даних	Ключові/сильні сторони	Основні обмеження	Типові сценарії використання
SIEM	Кореляція подій безпеки, формування цілісної картини інцидентів	Збір логів з усіх систем, виявлення складних ланцюжків атак, звітність, форензика	Висока складність впровадження, потреба у кваліфікованих аналітиках	Централізований моніторинг, аналіз інцидентів, підтримка розслідувань
SOAR	Автоматизація та оркестрація реагування на інциденти	Швидка реакція, стандартизовані плейбуки, зменшення навантаження на команди безпеки	Потребує ретельної розробки сценаріїв, залежить від якості вхідних сигналів	Автоматичне блокування акаунтів, ізоляція хостів, сповіщення, архівування артефактів, оновлення політик
Data Governance	Управління політиками, власністю та життєвим циклом даних	Формалізація правил, визначення власників, каталогізація, lineage, підтримка комплаєнсу	Не виконує технічний захист сам по собі, потребує інтеграції з інструментами безпеки	Розробка політик DLP, класифікації даних, регламентів доступу, підтримка відповідності GDPR, HIPAA, PCI DSS

Узагальнюючи проведений аналіз, можна зробити кілька принципових

висновків. По-перше, сучасні технології запобігання витоку даних формують багаторівневу, сильно інтегровану екосистему, в якій жодне рішення не є самодостатнім. DLP-платформи виконують роль ядра, фокусуючись на контролі контенту й контексту операцій із даними, але їхня максимальна ефективність досягається лише у поєднанні з CASB, DSPM, UEBA, DAM, IRM/DRM, SIEM/SOAR та іншими класами.

По-друге, ринок рішень є структурно диференційованим: навіть у межах одного класу (DLP, CASB, UEBA тощо) продукти суттєво відрізняються за архітектурою, глибиною аналізу, фокусом на локальні чи хмарні середовища, рівнем автоматизації та зручністю адміністрування. Це означає, що вибір платформи має базуватися на реальному профілі даних, бізнес-процесів та регуляторних вимог конкретної організації, а не лише на позиції в аналітичних рейтингах.

По-третє, ключовим фактором успіху є не стільки окремі технічні характеристики продуктів, скільки узгодженість їхньої роботи в єдиній моделі управління даними. Саме інтеграція DLP з хмарними, поведінковими, базовими й криптографічними інструментами, підкріплена процесами Data Governance та автоматизованим реагуванням SIEM/SOAR, дозволяє перейти від реактивного реагування на витоки до превентивного їх запобігання на рівні проєктування інформаційних систем і організаційних процесів.

По-четверте, для організацій різного масштабу оптимальні комбінації рішень будуть відрізнятися. Великі корпорації з розгалуженою мультихмарною інфраструктурою потребують комплексних DLP-рішень з потужними інтеграційними можливостями та окремими компонентами CASB, DSPM, UEBA й DAM. Організації середнього розміру частіше обирають більш інтегровані платформи (наприклад, DLP+CASB+IRM в межах однієї хмарної екосистеми) із меншими вимогами до адміністрування.

Таким чином, аналіз існуючих рішень показує, що роль DLP у сучасних системах захисту від витоку даних є системоутворюючою, але не ізольованою: саме через DLP реалізується значна частина політик контролю руху інформації, а успіх

впровадження залежить від того, наскільки вдало ці рішення інтегровані з іншими засобами та наскільки чітко організація визначила власні вимоги до безпеки даних. Це створює основу для подальших розділів роботи, у яких доцільно перейти від теорії до практики.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДАНИХ НА БАЗІ СУЧАСНОГО DLP РІШЕННЯ

2.1 Призначення та основні функції рішення DLP

У сучасних цифрових організаціях дані перестали бути другорядним ресурсом і перетворилися на ключовий елемент управління, конкурентоспроможності й розвитку. Це призвело до того, що вимоги до їхнього захисту зросли багатократно, а традиційні підходи, засновані на охороні периметра або ізоляції систем, виявилися недостатніми. У таких умовах рішення класу Data Loss Prevention (DLP) стали фундаментальним інструментом, який забезпечує безперервний, контекстно орієнтований і контентно залежний контроль над тим, як обробляється, передається, копіюється та використовується корпоративна інформація. Призначення DLP-систем полягає не лише у виявленні спроб ексфільтрації даних, але й у створенні масштабного механізму синхронізованого управління потоками інформації — такого, що забезпечує прозорість, запобігання інцидентам, реагування у реальному часі та дотримання регуляторних вимог.

Головною особливістю DLP є її орієнтація саме на дані як об'єкт захисту, а не на мережу, користувача чи інфраструктуру. Вона відстежує, що саме міститься у файлах або повідомленнях, у якому контексті здійснюються операції з інформацією, які умови доступу діють, які зразки поведінки є типовими для конкретних працівників, і чи не відхиляється поточна активність від дозволеної моделі. Такий підхід відрізняє DLP від рішень класу EDR, SIEM, CASB чи DAM, які контролюють системи, події чи поведінку, але не мають настільки глибокого доступу до вмісту. Забезпечення аналізу саме на рівні контенту — основна причина, чому DLP у багаторівневих архітектурах безпеки виступає як «останній

бар'єр», який дає змогу зупинити витік навіть тоді, коли інші захисні механізми не змогли виявити аномалію.

Призначення DLP-систем охоплює три стратегічні напрями: моніторинг, запобігання та реагування. Моніторинг забезпечує повну видимість руху даних у межах організації: які типи інформації обробляються, куди вони переміщуються, у якому вигляді передаються та чи відповідає це внутрішнім політикам. Запобігання передбачає блокування або обмеження дій, що можуть призвести до витоку: відправлення конфіденційного документа на зовнішню поштову адресу, копіювання службових файлів на USB-носії, завантаження технічної документації у публічні хмарні сховища чи масове архівування даних з ознаками підготовки до ексфільтрації. Реагування полягає у швидкому втручанні у разі інциденту: система може сповістити керівника, заблокувати дію, створити звіт, передати інформацію до SIEM чи навіть активувати автоматичні сценарії SOAR, що дозволяє негайно зупинити потенційний витік.

Ще однією критично важливою функцією DLP є підтримка нормативної відповідності. Сучасні регуляторні акти — такі як GDPR, NIS2, HIPAA, SOX, PCI DSS та державні стандарти — вимагають чіткої класифікації даних, контролю доступів, журналювання, механізмів запобігання передаванню персональної та фінансової інформації за неналежними каналами. DLP у цьому контексті виконує роль автоматизованого інструмента, який безперервно контролює дотримання політик і знижує ризик штрафів, судових позовів чи втрати репутації.

Цінність DLP-систем також полягає в інтеграції з іншими засобами безпеки. Вони можуть взаємодіяти з CASB для контролю хмарних сервісів, з DSPM — для виявлення критичних даних у хмарі, з UEBA — для аналізу поведінки користувачів, з DAM — для контролю доступу до баз даних, з EDR/XDR — для виявлення шкідливої активності, з SIEM/SOAR — для кореляції подій і автоматизованого реагування. Така інтеграція дозволяє DLP бути частиною екосистеми Zero Trust, де кожна дія з даними перевіряється відповідно до її контексту та ризикового профілю.

В основі роботи DLP лежить багаторівнева модель аналізу, що включає

контентний, контекстний та поведінковий підходи. Контентний аналіз забезпечує розпізнавання конфіденційної інформації у файлах, документах, базах даних, зображеннях, архівах та потоках даних. Це досягається за допомогою регулярних виразів, шаблонів, лінгвістичних моделей, цифрових відбитків, машинного навчання та засобів семантичного аналізу. Контекстний аналіз встановлює умови, за яких відбувається дія: хто її виконує, з якого пристрою, у який час, через який канал, до якого ресурсу та з якими правами доступу. Поведінковий аналіз оцінює типові моделі роботи користувача, виявляючи нетипові відхилення, що можуть свідчити про інсайдерську активність або компрометацію облікового запису.

Однією з ключових особливостей сучасних DLP-рішень є використання штучного інтелекту. Машинне навчання дає можливість зменшити кількість хибнопозитивних спрацьовувань, точніше класифікувати дані, аналізувати складні документи, такі як технічні креслення, фінансові звіти чи медичні картки, а також виявляти аномалії в реальному часі. У найбільш просунутих системах ML-моделі будуються окремо для кожного бізнес-процесу, що дозволяє адаптувати політики під унікальні особливості організації. З практичної точки зору функціональні можливості DLP можна умовно розділити на кілька груп: контроль каналів, контроль кінцевих точок, захист у хмарних середовищах, аналіз файлів і потоків даних, управління політиками, реагування на інциденти та звітність. Контроль каналів охоплює електронну пошту, веб-трафік, FTP/SFTP, месенджери, API-взаємодії, друк та фізичні носії. На рівні кінцевих точок DLP контролює копіювання, перейменування, архівування, створення скриншотів, запис на USB-носії, підключення зовнішніх пристроїв. У хмарних середовищах DLP інтегрується з API платформ Microsoft 365, Google Workspace, Salesforce, AWS, Azure та інших сервісів для контролю дій користувачів і документів.

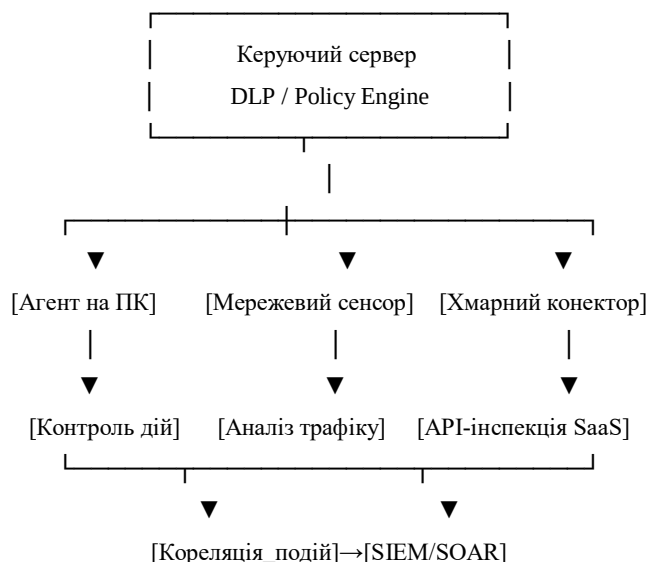


Рис.2.1. Взаємодія компонентів DLP у корпоративному середовищі

У сучасних умовах функціональність DLP-рішень виходить далеко за межі простого виявлення забороненого контенту та його блокування. DLP стає системою стратегічного значення, яка забезпечує багаторівневий, контекстно-чутливий та адаптивний контроль над даними на всіх етапах їхнього життєвого циклу, охоплюючи як статичні, так і динамічні інформаційні потоки. Одним із ключових аспектів ефективності DLP є здатність інтегруватися з бізнес-процесами без зниження продуктивності користувачів. У сучасних організаціях обробка інформації є високодинамічним процесом, тому DLP повинна працювати у фоновому режимі, забезпечуючи безпеку непомітно для співробітників, але водночас оперативно реагувати на порушення. Це вимагає високої точності аналізу, оскільки надмірна кількість хибних спрацювань призводить до зниження довіри до системи, ускладнення операційної діяльності та інколи навіть до відключення окремих політик.

Завдяки комплексному моніторингу DLP створює повну картину взаємодії користувачів з інформацією: які файли вони відкривають, які програми

використовують, як переміщують дані, чи відправляють їх через зовнішні сервіси, чи використовують зашифровані канали. Це дозволяє формувати поведінкові моделі для кожного користувача та визначати відхилення від нормальної активності. Наприклад, якщо співробітник протягом року працював здебільшого з фінансовою документацією, але раптово починає копіювати великі обсяги інженерних креслень, система сприймає це як аномалію та ініціює додаткову перевірку. Такі механізми дозволяють виявляти інциденти на ранніх етапах, ще до моменту фактичної ексфільтрації.

Функції контентного та контекстного аналізу, які виконують DLP-рішення, дають змогу враховувати сотні параметрів під час оцінювання ризику. До контентних методів належать шаблонне розпізнавання, машинне навчання, *fingerprinting* і різні механізми семантичного аналізу, які дозволяють визначати наявність конфіденційної інформації навіть у складних структурах. Наприклад, технологія *fingerprinting* створює унікальний хеш-код документа або набору даних, що дозволяє виявляти витoki навіть у разі часткової модифікації файлу. Контекстний аналіз включає розуміння того, хто є ініціатором операції, у якому середовищі вона відбувається, через який канал здійснюється передавання, до яких груп належить користувач, який рівень довіри має пристрій, яким є час доби та інші релевантні фактори.

У практичних умовах контентно-контекстне оцінювання допомагає DLP приймати рішення з високим рівнем точності. Наприклад, відправлення документа з конфіденційною інформацією на корпоративну електронну адресу може бути дозволеним, у той час як спроба відправити цей самий документ через веб-пошту Gmail буде одразу заблокована. Такої гнучкості неможливо досягти без глибокого аналізу контексту, що включає визначення типу каналу, ступеня довіри до нього, політик організації та типових моделей поведінки користувача.

Важливою функцією DLP-рішень є контроль за каналами передачі інформації. Сучасні системи охоплюють як класичні канали (електронна пошта, мережеві протоколи, USB-пристрої), так і новітні (SaaS-застосунки, API, мобільні додатки, корпоративні месенджери). Завдяки цьому забезпечується наскрізна

видимість руху даних. У межах контролю каналів DLP здійснює перевірку інформації у момент її передачі, що називається inline-контролем. Inline-механізми дають змогу блокувати заборонені операції ще до того, як дані залишать периметр організації. Наприклад, якщо користувач намагається завантажити файл із фінансовими звітами у свій особистий хмарний сервіс, система може автоматично зупинити передачу і попередити користувача про порушення політики.

DLP також має важливу роль у захисті даних у стані спокою (data-at-rest). Це стосується файлових сховищ, мережевих директорій, локальних пристроїв і корпоративних репозиторіїв. За допомогою періодичного чи постійного сканування DLP ідентифікує файли, які містять конфіденційну інформацію, але зберігаються у невідповідних місцях, наприклад у загальних папках із широкими правами доступу. Функція виявлення даних у стані спокою дозволяє організаціям значно зменшити ризики випадкових витоків, спричинених недостатньою сегментацією або неусвідомленими діями співробітників.

Контроль даних у стані використання (data-in-use) включає нагляд за діями користувачів у реальному часі: копіюванням, відкриттям, друком, створенням скріншотів, вставленням через буфер обміну або архівуванням. Це найбільш складний тип контролю, оскільки такі дії не завжди супроводжуються передаванням інформації через мережу. Для цього DLP використовує спеціальні механізми на рівні операційної системи, що дозволяють перехоплювати системні виклики і застосовувати політики до кожної окремої операції. Наприклад, якщо користувач робить спробу вставити конфіденційний фрагмент тексту у сторонній чат, система може замінити вміст на порожній текст і згенерувати сповіщення.

У межах DLP-архітектури важливе місце займає логування та формування звітності. Сучасні системи фіксують кожну дію з даними — навіть ті, що не призводять до порушень. Це дозволяє організації отримувати детальну картину інформаційних потоків, виявляти приховані ризики та аналізувати поведінкові патерни. Інтеграція з SIEM сприяє кореляції подій і формуванню комплексного розуміння інцидентів, а системи SOAR забезпечують часткову або повну

автоматизацію реагування. Наприклад, якщо DLP фіксує серію аномальних дій у нічний час із використанням потенційно скомпрометованого облікового запису, SOAR може автоматично заблокувати користувача, повідомити службу безпеки, згенерувати тикет і зібрати необхідну інформацію для цифрової експертизи.

Суттєвою складовою функціональності DLP є класифікація даних, яка може здійснюватися вручну, автоматично або в комбінованому режимі. Автоматична класифікація базується на аналізі вмісту та структури документа, виявленні характерних шаблонів, метаданих, ключових слів, контекстів використання та інших факторів. У сучасних системах застосовуються алгоритми машинного навчання, здатні визначати тип документа навіть у разі відсутності очевидних індикаторів. Завдяки цьому класифікація стає незалежною від людського фактора і значно точнішою. Наприклад, система може автоматично розпізнати, що документ містить персональні дані, навіть якщо він поданий у нестандартному форматі або якщо текст приховано в таблицях чи зображеннях.

У межах функції класифікації особливого значення набувають механізми Data Tagging і Data Labeling. Даним присвоюються спеціальні мітки, які супроводжують їх у процесі зберігання, передачі та обробки. Ці мітки можуть містити інформацію про рівень конфіденційності, правила доступу, строки зберігання, наявність персональних даних і допустимі операції. Такі мітки не лише дозволяють DLP застосовувати відповідні політики, а й забезпечують прозорість управління інформацією у масштабі всієї організації.

Особливо значущою є функція запобігання інсайдерським загрозам. DLP аналізує дії користувачів, їх робочі патерни і типові сценарії взаємодії з даними. Якщо співробітник починає поводитися нетипово — наприклад, масово копіювати файли, завантажувати велику кількість документів у персональні сервіси або змінювати структуру критичних файлових каталогів — система фіксує відхилення і визначає ризиковість дій. Такі механізми дозволяють організаціям виявляти внутрішні загрози ще до того, як відбудеться ексфільтрація даних. Це особливо важливо для великих компаній, де внутрішні зловживання можуть призвести до значних збитків.

DLP також виконує функцію контролю відповідності нормативним вимогам. У сфері захисту інформації діють численні міжнародні та локальні стандарти — GDPR, HIPAA, PCI DSS, ISO 27001, SOC 2 та інші. DLP допомагає організаціям документувати і підтверджувати дотримання вимог, формувати звіти для аудиторів, забезпечувати контроль над персональними даними та критично важливою інформацією. Наприклад, GDPR вимагає, щоб організації забезпечували захист персональних даних на всіх етапах обробки, а також мали можливість повідомляти про інциденти у встановлені строки. Системи DLP надають інструменти для виконання цих вимог — від автоматизованої класифікації персональних даних до журналювання і контролю операцій з ними.

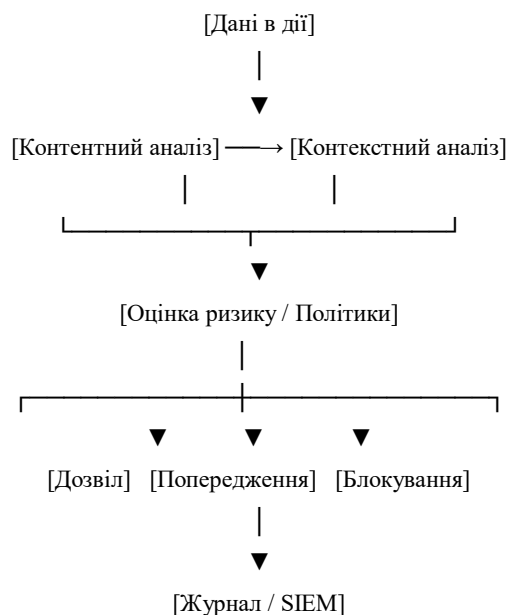


Рис.2.2. Робота DLP у контексті багаторівневого аналізу:

У практиці застосування DLP відіграє критично важливу роль у формуванні культури безпеки. Система не лише блокує порушення, а й навчає користувачів коректним діям. Коли співробітник отримує сповіщення про те, що передача файлу порушує політику організації, він поступово адаптує свою поведінку відповідно до вимог безпеки. Це допомагає зменшити кількість інцидентів, пов'язаних із людським фактором, та підвищує загальний рівень інформаційної грамотності персоналу.

У перспективі функціональність DLP продовжує розширюватися за рахунок

інтеграції з технологіями штучного інтелекту, машинного навчання, поведінкового аналізу та прогнозування ризиків. Алгоритми починають передбачати можливі інциденти, аналізуючи не лише поточні дії користувачів, а й довготривалі тенденції. Це дозволяє переходити від реактивного до проактивного управління безпекою — коли система запобігає інцидентам ще до моменту їхнього виникнення.

У сучасних умовах, коли організації активно переходять до гібридних і розподілених інфраструктур, DLP-рішення виконують важливу функцію забезпечення контролю за інформацією поза традиційним периметром. Мобільність співробітників, широке використання хмарних сервісів та персональних пристроїв роблять класичні механізми безпеки недостатніми, тоді як DLP-агенти забезпечують постійний нагляд за даними незалежно від місця перебування користувача. Завдяки цьому організація отримує можливість підтримувати високий рівень безпеки навіть у випадках, коли частина процесів відбувається в непередбачуваних або потенційно небезпечних умовах.

Важливу роль у функціонуванні DLP відіграють механізми шифрування, які автоматично застосовуються до даних відповідно до їх типу, змісту та рівня чутливості. Шифрування дозволяє запобігти доступу до інформації навіть у випадку її викрадення, втраченого пристрою або компрометації хмарного середовища. У поєднанні з функціями класифікації це створює комплексну систему, у якій кожен тип даних супроводжується відповідними правилами захисту. Наприклад, комерційні таємниці, персональні дані або фінансова звітність можуть бути автоматично зашифровані на момент створення документа, що унеможлиблює їх прочитання сторонніми програмами або сервісами.

DLP також відіграє ключову роль у виявленні та блокуванні сучасних методів обфускації даних. У багатьох випадках зловмисники намагаються уникнути виявлення за допомогою шифрування файлів, упакування архівів у кілька шарів, використання нестандартних символів або зміни структури документів. Сучасні DLP-рішення оснащені механізмами декодування, структурного аналізу, OCR-розпізнавання тексту та виявлення прихованих

патернів, що дозволяє виявляти конфіденційні дані навіть у складних і нетипових форматах. Завдяки цьому організація отримує можливість виявляти витoki на ранньому етапі, ще до того, як злоумисник встигне передати інформацію за межі корпоративного середовища.

У багатьох випадках функціональність DLP дозволяє попереджати інциденти, пов'язані з використанням сторонніх хмарних сервісів, які не контролюються політиками організації. Працівники часто завантажують файли у персональні Google Drive, Dropbox або інші сервіси, не усвідомлюючи, що це створює серйозні ризики для цілісності інформаційних активів. DLP автоматично визначає такі сценарії та блокує невідповідні дії. У випадках, коли хмарні сервіси використовуються для легітимних бізнес-процесів, система аналізує умови передачі, оцінює довіреність каналу та наявність відповідних маркерів безпеки.

Сучасні DLP-рішення також активно застосовуються у рамках моделі Zero Trust, яка передбачає відсутність довіри до будь-якого користувача або пристрою без постійної перевірки. У цьому контексті DLP стає одним із ключових механізмів контролю, який доповнює автентифікацію, авторизацію та контроль привілеїв. DLP аналізує, чи відповідає дія користувача його ролі, чи не виходить вона за межі дозволеної моделі поведінки, чи є спроба доступу до даних легітимною в поточному контексті. Наприклад, навіть якщо користувач проходить багатофакторну автентифікацію, його спроба завантажити великий масив даних у невідомий хмарний ресурс може бути заблокована через невідповідність загальним політикам організації.

У практиці застосування DLP особливо важливою є здатність системи адаптуватися до змін у поведінці користувачів та загальній динаміці роботи організації. Це забезпечується інтелектуальними алгоритмами, які формують моделі нормальної активності та визначають відхилення, що можуть свідчити про інциденти або потенційні загрози. Машинне навчання дозволяє системі постійно вдосконалюватися та зменшувати кількість хибнопозитивних спрацювань, що підвищує точність аналізу та ефективність усіх механізмів контролю. У той самий час така адаптивність робить DLP важливим інструментом для виявлення нових,

раніше невідомих сценаріїв ексфільтрації даних.

Однією з характерних рис сучасних DLP-систем є можливість масштабування відповідно до потреб організації. Це дозволяє використовувати їх як у малих підприємствах, де обсяги даних обмежені, так і у великих корпораціях із розподіленою інфраструктурою. Масштабованість забезпечується завдяки архітектурі, заснованій на агентах, хмарних конекторах, мережевих сенсорах і централізованих аналітичних платформах. Кожен компонент може бути розгорнутий незалежно, що дозволяє адаптувати систему відповідно до специфіки бізнес-процесів та рівня ризику в конкретному середовищі.

Суттєвим елементом функціональності DLP є можливість проведення цифрової експертизи (forensics). У разі інциденту система дозволяє відтворити шлях проходження даних, визначити користувача, час дії, використовуваний канал, тип документа та інші важливі параметри. Це дає змогу швидко встановити причину інциденту, оцінити його масштаб і визначити подальші кроки з відновлення безпеки. У деяких системах передбачено функціонал відкату дій, який дозволяє блокувати доступ до скомпрометованих даних або повертати їх у вихідний стан.

Крім того, важливою функцією DLP є підтримка процесів аудиту та внутрішнього контролю. Завдяки можливості формування детальних звітів система допомагає аудиторам оцінити рівень відповідності вимогам безпеки, перевірити виконання політик, проаналізувати історію інцидентів і визначити слабкі місця в інфраструктурі. Це сприяє вдосконаленню загальної системи управління ризиками та розробці заходів для запобігання майбутнім порушенням.

У контексті управління життєвим циклом даних DLP виконує функцію контролю за правильністю зберігання та видалення інформації. Невідповідна утилізація даних є одним із найпоширеніших джерел витоків: файли можуть залишатися у відкритих каталогах, кешах браузерів, тимчасових папках або хмарних сервісах. DLP дозволяє визначити такі об'єкти, позначити їх як ризикові та застосувати до них політики очищення або перенесення у захищені репозиторії. Це забезпечує безпеку даних на всіх етапах їхнього існування в організації.

Ще однією ключовою функцією сучасних DLP-систем є інтеграція з системами управління привілеями. Завдяки цьому можна відстежувати, як користувачі з різними рівнями доступу взаємодіють із конфіденційною інформацією. Це особливо важливо для контролю доступу до найбільш критичних даних, робота з якими повинна бути обмежена лише тими працівниками, які дійсно потребують їх для виконання своїх обов'язків. У разі виявлення порушень доступ може бути автоматично заблокований, а інцидент — передано на розгляд службі безпеки.

Підсумовуючи, можна стверджувати, що функції сучасних DLP-рішень формують комплексну систему безпеки, яка охоплює всі аспекти роботи з даними: їх створення, зберігання, переміщення, копіювання, обробку та видалення. DLP забезпечує наскрізний контроль інформаційних потоків, мінімізує ймовірність помилок користувачів, блокує зловмисні дії, виявляє внутрішні загрози, підтримує нормативну відповідність та створює фундамент для формування культури безпеки в організації. Завдяки інтеграції з інтелектуальними алгоритмами аналізу поведінки та машинним навчанням DLP стає одним із найважливіших інструментів захисту інформаційних активів у сучасних умовах цифрової трансформації.

Суттєвим елементом функціональності DLP є можливість проведення цифрової експертизи (forensics). У разі інциденту система дозволяє відтворити шлях проходження даних, визначити користувача, час дії, використовуваний канал, тип документа та інші важливі параметри. Це дає змогу швидко встановити причину інциденту, оцінити його масштаб і визначити подальші кроки з відновлення безпеки. У деяких системах передбачено функціонал відкату дій, який дозволяє блокувати доступ до скомпрометованих даних або повертати їх у вихідний стан.

Крім того, важливою функцією DLP є підтримка процесів аудиту та внутрішнього контролю. Завдяки можливості формування детальних звітів система допомагає аудиторам оцінити рівень відповідності вимогам безпеки, перевірити виконання політик, проаналізувати історію інцидентів і визначити

слабкі місця в інфраструктурі. Це сприяє вдосконаленню загальної системи управління ризиками та розробці заходів для запобігання майбутнім порушенням.

У контексті управління життєвим циклом даних DLP виконує функцію контролю за правильністю зберігання та видалення інформації. Невідповідна утилізація даних є одним із найпоширеніших джерел витоків: файли можуть залишатися у відкритих каталогах, кешах браузерів, тимчасових папках або хмарних сервісах. DLP дозволяє визначити такі об'єкти, позначити їх як ризикові та застосувати до них політики очищення або перенесення у захищені репозиторії. Це забезпечує безпеку даних на всіх етапах їхнього існування в організації.

Ще однією ключовою функцією сучасних DLP-систем є інтеграція з системами управління привілеями. Завдяки цьому можна відстежувати, як користувачі з різними рівнями доступу взаємодіють із конфіденційною інформацією. Це особливо важливо для контролю доступу до найбільш критичних даних, робота з якими повинна бути обмежена лише тими працівниками, які дійсно потребують їх для виконання своїх обов'язків. У разі виявлення порушень доступ може бути автоматично заблокований, а інцидент — передано на розгляд службі безпеки.

Підсумовуючи, можна стверджувати, що функції сучасних DLP-рішень формують комплексну систему безпеки, яка охоплює всі аспекти роботи з даними: їх створення, зберігання, переміщення, копіювання, обробку та видалення. DLP забезпечує наскрізний контроль інформаційних потоків, мінімізує ймовірність помилок користувачів, блокує зловмисні дії, виявляє внутрішні загрози, підтримує нормативну відповідність та створює фундамент для формування культури безпеки в організації. Завдяки інтеграції з інтелектуальними алгоритмами аналізу поведінки та машинним навчанням DLP стає одним із найважливіших інструментів захисту інформаційних активів у сучасних умовах цифрової трансформації.

2.2 Основні компоненти загальної архітектури DLP

Сучасні рішення класу Data Loss Prevention формуються як багаторівневі та розподілені системи, архітектура яких об'єднує різні технологічні компоненти, відповідальні за контроль даних у всіх станах — під час створення, у процесі передачі, зберігання та використання. На відміну від класичних систем кіберзахисту, які орієнтуються передусім на події, інфраструктуру або поведінку шкідливого коду, DLP працює безпосередньо з інформацією як з основним об'єктом, і тому потребує складної інтеграції між серверами політик, аналітичними механізмами, агентами кінцевих точок, мережевими сенсорами, хмарними конекторами та службами кореляції інцидентів. Архітектура системи залишається ключовим фактором її ефективності, оскільки саме від того, як взаємодіють окремі компоненти, залежить глибина аналізу, точність виявлення витоків, швидкість реагування, а також масштабованість та безперервність роботи в умовах гібридної інфраструктури.

У загальному вигляді архітектура DLP розглядається як багат шарова модель, що складається з рівня керування, рівня виявлення та примусового контролю, рівня класифікації даних, рівня інтеграцій та сервісів з обробки метаданих. Центральним ядром системи виступає керуючий сервер — Policy Server або Management Server, — який зберігає політики, правила доступу, конфігурації агентів, журнали інцидентів та шаблони класифікації. Саме на цьому рівні формується логіка реагування, визначаються умови дозволених та заборонених дій, конфігурується ризиковий профіль користувачів, а також здійснюється кореляція подій і оцінка контексту. Центральний сервер взаємодіє з корпоративними каталогами, такими як Active Directory або Azure AD, а також із SIEM- та SOAR-платформами, які отримують фінальні інциденти та забезпечують додатковий рівень автоматизації. Його роль є критичною: у великих компаніях саме цей компонент стає центром управління всією інформаційною безпекою, дозволяючи інтегрувати DLP у загальну модель Zero Trust та забезпечувати наскрізний контроль за всіма інформаційними потоками.

Робота центрального серверу неможлива без репозитарію даних, який забезпечує зберігання інцидентів, політик, цифрових відбитків документів,

журналів та службових подій. У класичних реалізаціях, таких як Symantec DLP або Forcepoint DLP, застосовуються окремі сховища, оптимізовані для роботи з великим масивом структурованої інформації, що дозволяє швидко виконувати пошук, кореляцію та аналіз. Репозитарій також відіграє важливу роль у процесі судової експертизи (digital forensics), оскільки містить повний контекст інциденту, включно з метаданими файлу, діями користувача та умовами, за яких було виявлено порушення. Таким чином, серверна частина архітектури забезпечує аналітичний центр системи, де перетинаються всі події з різних каналів, а рішення щодо реагування, блокування чи дозволу операцій формуються на основі складної логіки, поєднуючи контентний, контекстний та поведінковий аналізи.

Найбільш розгалуженим компонентом DLP є рівень детекторів — елементів, що здійснюють аналіз і контроль безпосередньо там, де відбувається робота з даними. Першим і найважливішим серед них є агент кінцевої точки (Endpoint DLP Agent), який працює на комп'ютерах користувачів і забезпечує контроль інформації у стані використання. На рівні операційної системи агент перехоплює системні виклики, що стосуються доступу до файлів, копіювання, переміщення, друку, створення скріншотів, передачі через буфер обміну або вставлення даних у сторонні додатки. Його архітектура включає драйвери ядра, служби моніторингу, локальні кеші політик та механізми обмеження операцій. Саме завдяки агенту система може блокувати дії ще до того, як дані будуть передані за межі пристрою, що робить його ключовим елементом для запобігання інсайдерським загрозам. Динамічні моделі поведінкового аналізу дозволяють агентам адаптуватися до звичайної активності користувача, виявляючи нетипові відхилення та попереджаючи потенційні спроби ексфільтрації.

У розподілених корпоративних мережах важливим компонентом архітектури виступають мережеві сенсори, або Network DLP, які працюють на рівні контролю інформації в русі. Вони інтегруються у мережеву інфраструктуру через SPAN-порти, TAP-сенсори або шлюзи електронної пошти та веб-трафіку. Мережеві детектори виконують глибинну інспекцію пакетів (DPI), аналізують вкладення електронної пошти, передані файли, HTTP(S)-трафік, FTP-сеанси та

будь-які інші канали, через які може відбуватися передавання інформації. Контентний аналіз на мережевому рівні складніший, оскільки вимагає розшифрування трафіку, але сучасні системи інтегруються з TLS-Inspection, забезпечуючи можливість аналізу шифрованих потоків. Мережевий рівень є особливо важливим у тих сценаріях, де організація має змішані або застарілі системи, що не підтримують агентів, але використовують стандартні комунікаційні протоколи.

Зі зростанням використання хмарних сервісів окремим і невід’ємним компонентом DLP стали хмарні конектори та API-контролери, які працюють у середовищах Microsoft 365, Google Workspace, Salesforce, Box, AWS, Azure та інших SaaS-платформах. Їх завданням є контроль операцій, які відбуваються без участі локального пристрою користувача, а саме: переміщення файлів у хмарні сховища, їх поширення через посилання, робота у документах онлайн, використання сторонніх застосунків, що інтегруються через API. Хмарні DLP-компоненти аналізують як вміст документів, так і метадані доступу, дозволяючи запобігати витокам, що виникають через неправильні налаштування доступів, відкриті посилання, сторонні додатки або неконтрольовані інтеграції. На відміну від мережевих сенсорів, які перехоплюють трафік, хмарні конектори працюють безпосередньо з API, що забезпечує вищу точність і незалежність від мережевої інфраструктури.

Усі зазначені компоненти пов’язуються у єдину систему за допомогою аналітичних модулів класифікації даних та контентного аналізу. Ці модулі включають регулярні вирази, пошук шаблонів, цифрові відбитки документів (fingerprinting), Exact Data Match, Document Matching, OCR-аналіз графічних файлів, лінгвістичні моделі та алгоритми машинного навчання. Вони працюють на всіх рівнях — у агенті, на сервері, у хмарному конекторі, у мережевому сенсорі. Класифікаційний модуль може бути централізований, але більшість сучасних систем дублюють частину логіки локально, щоб забезпечити швидкість ухвалення рішень у реальному часі.

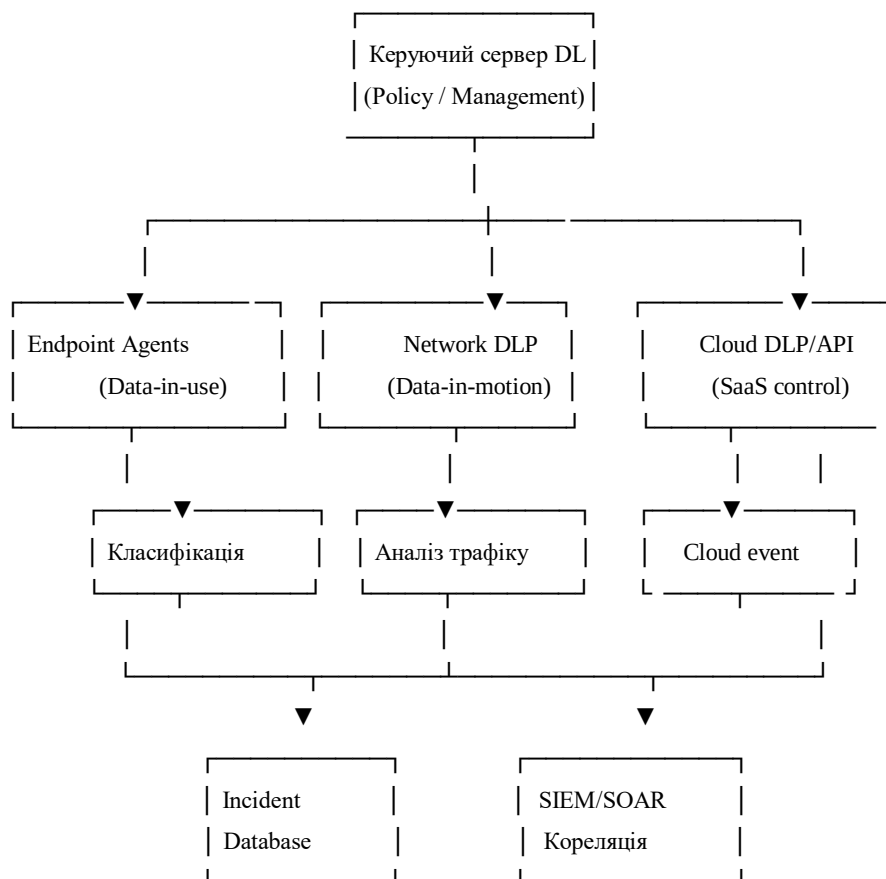


Рис.2.3. Типова DLP-архітектура

Архітектурна модель DLP доповнюється системами інтеграції, які дозволяють передавати інформацію до зовнішніх джерел та інструментів безпеки. SIEM-системи отримують структуровані інциденти, включаючи деталі операцій, класифікацію файлу, дії користувача та рішення, прийняті DLP. SOAR-платформи забезпечують автоматизацію реагування — блокування облікового запису, ескалацію порушення, створення службових заявок, ізоляцію пристрою або запуск цифрової експертизи. Інтеграція з IAM-системами забезпечує коректну ідентифікацію користувача, тоді як зв'язок із системами управління привілеями дозволяє застосовувати політики відповідно до ролей і рівнів доступу.

Важливою частиною архітектури DLP є підтримка класифікації даних на

всіх етапах життєвого циклу. Сучасні рішення інтегрують автоматичне маркування документів, додавання службових тегів, вбудовування метаданих, що містять рівень конфіденційності та правила обробки. Такі метадані супроводжують файл незалежно від того, де він перебуває — на кінцевій точці, у хмарному сховищі чи у мережевому каналі. Це дозволяє системі застосовувати політики навіть у тих випадках, коли файл був переміщений у нове середовище або змінений користувачем.

З огляду на зростання мобільності, важливою складовою DLP-архітектури є підтримка гібридного та віддаленого доступу. Агенти повинні працювати автономно навіть без зв'язку з сервером, зберігаючи локальні політики та правила. Після відновлення підключення агент синхронізується з центральним сервером та передає журнали. Такий підхід забезпечує безпеку в умовах гнучких робочих моделей, коли співробітники можуть працювати з будь-якого пристрою та мережі.

Системи DLP також включають компоненти аналізу ризику та поведінкового профілювання. Використовуючи UEBA-алгоритми, система може аналізувати дії користувачів, визначаючи, наскільки вони відповідають типовому патерну поведінки. Нетипові дії — масове копіювання файлів, нічна активність, доступ до нетипових ресурсів — підвищують ризиковий бал і можуть призвести до автоматичного блокування дії або ескалації інциденту.

Архітектура DLP також передбачає використання спеціалізованих модулів для аналізу даних у стані спокою, що забезпечується механізмами періодичного або постійного сканування файлових сховищ, серверних каталогів, локальних дисків та хмарних репозиторіїв. Такі модулі дозволяють виявити конфіденційну інформацію, яка зберігається у невідповідних місцях або має неправильні права доступу. Для великих корпорацій, де історично накопичено значні обсяги документів, функціональність Data-at-Rest Discovery стає основою для запровадження політик класифікації та підвищення безпеки інфраструктури. Деякі реалізації підтримують інкрементальне сканування, що дозволяє аналізувати лише нові та змінені файли, значно зменшуючи навантаження на

системні ресурси та прискорюючи процес розгортання.

Важливе місце в DLP-архітектурі займає система управління політиками. Вона не лише зберігає правила, а й забезпечує механізм їхнього поширення до всіх компонентів системи. Політики можуть містити десятки параметрів: типи контенту, рівень конфіденційності, дозволені та заборонені канали, групи користувачів, контекстні умови, винятки, часові обмеження та ризикові категорії. Для того щоб система залишалася узгодженою в масштабі всієї організації, сервер управління повинен коректно синхронізувати політики з агентами та мережевими модулями, забезпечуючи їхню актуальність незалежно від того, чи користувач працює локально або віддалено. Багато сучасних рішень підтримують динамічне оновлення політик без перезавантаження агентів, що дозволяє змінювати правила практично в реальному часі.

Ще одним системним елементом є механізм цифрових відбитків (fingerprinting), який дозволяє створювати унікальні сигнатури документів, таблиць, баз даних або специфічних наборів інформації. Така функція особливо актуальна у випадках, коли стандартний контент-аналіз недостатній — наприклад, при роботі з нестандартними форматами або при часткових модифікаціях файлів. Fingerprinting може базуватися як на структурі документа, так і на більш абстрактних паттернах, що дозволяє виявляти витoki навіть у разі зміни словоформ або перестановки фрагментів. Компонент цифрового відбитку інтегрується в усі елементи архітектури — від агента на робочій станції до хмарних модулів, забезпечуючи однаковий рівень точності незалежно від місця зберігання або передачі файлу.

Для повноцінної роботи системи важливою є комунікаційна інфраструктура, яка забезпечує обмін даними між сервером, агентами, сенсорами та хмарними компонентами. У більшості сучасних систем використовується захищений трафік з TLS-шифруванням, а передавання даних здійснюється пакетно, з урахуванням обмежень пропускної здатності мережі. Агент зберігає журнали локально та передає їх на сервер частинами, що дозволяє уникнути пікових навантажень. Для великих організацій важливим є розподілений режим,

коли використовується декілька серверів політик, балансування навантаження та географічна реплікація даних. Це дозволяє забезпечити безперебійність роботи навіть у разі збою окремих вузлів.

Ключову роль у DLP відіграє модуль прийняття рішень — Decision Engine, який може бути реалізований у вигляді локальної служби агента або централізованого компонента на сервері. Він визначає, яку дію потрібно виконати у відповідь на виявлене порушення: дозволити операцію, заблокувати її, відправити попередження користувачу, увімкнути детальніший режим моніторингу, змінити рівень ризику або передати інцидент у зовнішню систему. У складніших системах Decision Engine використовує комбінацію правил і моделей машинного навчання, що дозволяє приймати рішення не лише на основі статичних політик, а й урахувати поведінкові закономірності та контекст виконання дії.

Окремим напрямом архітектури є робота з API, яка дозволяє DLP взаємодіяти із зовнішніми сервісами, такими як корпоративні портали, системи електронного документообігу, платформи розробки, внутрішні CRM або ERP. Через API DLP отримує інформацію про документи, доступи, зміни у структурі організації, нові ролі користувачів, групи безпеки тощо. У великих компаніях API-інтеграції можуть охоплювати сотні застосунків, тому важливо, щоб архітектура DLP була достатньо гнучкою для роботи з різноманітними протоколами й форматами даних.

У сучасних системах дедалі більше уваги приділяється хмарно-орієнтованій архітектурі, де сервер політик може бути розгорнутий у вигляді SaaS-рішення. Це дозволяє знизити витрати на інфраструктуру, забезпечити регулярні оновлення та підвищити масштабованість. Водночас SaaS-рішення вимагають високого рівня довіри до постачальника, оскільки частина функцій — зокрема, обробка метаданих та аналіз інцидентів — виконується на сторонніх серверах. У таких випадках шифрування та політики ізоляції даних стають невід'ємною частиною архітектури.

Ще один важливий елемент — модулі локального кешування політик і

класифікаційних шаблонів на агентах. Вони забезпечують можливість автономної роботи у випадках нестабільного зв'язку або повної відсутності підключення. Кешування дозволяє агенту правильно реагувати на інциденти без звернення до центрального сервера, що є критично важливим у сценаріях віддаленої роботи. Після відновлення мережі агент передає журнали та синхронізує оновлені політики, не порушуючи цілісність системи.

Архітектура DLP також включає механізми стекового контролю, які дозволяють визначати порядок застосування політик залежно від пріоритетів. Наприклад, політики, що регулюють персональні дані, можуть мати вищий пріоритет порівняно з політиками, які стосуються внутрішніх документів. Це забезпечує більш точний контроль і дозволяє уникнути надмірних блокувань.

У контексті масштабованості важливим є використання контейнеризації та мікросервісних архітектур, які дають змогу ефективно розподіляти навантаження. Сучасні DLP-платформи дедалі частіше впроваджують Kubernetes-кластери для балансування трафіку та обробки великого обсягу даних, що робить систему стійкою до пікових навантажень і збоїв окремих вузлів.

Суттєвим технічним елементом архітектури DLP є механізм журналювання та реплікації подій. Оскільки система може обробляти тисячі інцидентів щоденно, важливо забезпечити надійне зберігання журналів, їхню реплікацію в резервні центри обробки даних та можливість швидкого доступу до них під час розслідувань. У розподілених організаціях журналювання може здійснюватися на декількох рівнях: локально на агенті, на проміжних серверах у філіях та на центральному сервері. Це дозволяє зменшити затримки в роботі, а також забезпечує безперервність збору журналів навіть у випадку тимчасової втрати зв'язку між вузлами.

Окремої уваги потребує модуль обробки інцидентів, який забезпечує їхню класифікацію, категоризацію, пріоритизацію та забезпечення workflow для команди кібербезпеки. Більшість сучасних DLP-рішень дозволяють налаштовувати автоматизовані сценарії: наприклад, якщо інцидент належить до високої категорії ризику, система може не лише блокувати операцію, а й

автоматично відкривати тікет у системі управління інцидентами, створювати повідомлення у корпоративному месенджері, надсилати alert на електронну пошту відповідальної особи або запускати інтегрований механізм SOAR для виконання скриптів реагування. Така автоматизація значно пришвидшує час реакції та зменшує ймовірність пропуску критичного інциденту.

Наступний важливий компонент — аналітична панель (dashboard) та система візуалізації. Оскільки DLP генерує великий обсяг інформації, потрібні інструменти для інтерактивного аналізу: виявлення трендів, пошуку аномалій, аналізу поведінкових патернів, порівняння різних періодів. Візуалізація допомагає не лише технічним фахівцям, а й керівництву, яке приймає стратегічні рішення на основі статистики. Аналітичні панелі можуть відображати рівень конфіденційності документів, активність користувачів, кількість блокувань за певний період, популярні канали ексфільтрації, навантаження на агенти, частоту спрацьовувань конкретних політик та інші показники, що дозволяють побачити повну картину інформаційної безпеки організації.

У контексті архітектури особливої уваги потребує взаємодія DLP із користувачами. Це включає механізми сповіщень, попереджень, навчальних підказок та повідомлень про порушення політик. Система може інформувати користувача про те, які саме правила він порушив, і рекомендувати альтернативні дії, що відповідають вимогам безпеки. Такий підхід не лише підвищує обізнаність працівників щодо політик безпеки, а й сприяє зменшенню кількості повторних інцидентів. У деяких системах передбачено можливість підтвердження дії користувачем, якщо операція знаходиться у «сірій зоні» — наприклад, коли документ містить чутливу інформацію, але все ж може бути переданий у рамках бізнес-процесу. У таких випадках система створює журнал винятку, що дозволяє надалі оцінювати адекватність поведінки працівника.

Архітектура DLP також включає можливості глибокої адаптації до специфіки бізнес-процесів. У корпоративних системах можуть існувати десятки унікальних потоків даних: обробка фінансової звітності, передавання юридичних документів, робота з персональними даними клієнтів, R&D-інформація, CAD-

моделі тощо. DLP має підтримувати можливість створення кастомних правил, що враховують терміни, обсяги, типи документів, формат файлів, характер бізнес-процесів та типи взаємодій із зовнішніми партнерами. У великих організаціях часто використовують профілі політик для різних підрозділів: юридичного відділу, фінансового департаменту, R&D-команди, маркетингу та відділу продажів. Це забезпечує високу точність контролю та дозволяє уникати зайвих блокувань, які можуть заважати роботі персоналу.

У хмарно-орієнтованих архітектурах важливими є модулі, що дозволяють DLP ідентифікувати та контролювати дані, які переміщуються між SaaS-платформами. Наприклад, обмін файлами між Microsoft 365, Slack і Salesforce може відбуватися без проходження через корпоративну інфраструктуру. У таких умовах класичний мережевий контроль стає неефективним. Хмарні DLP-конектори використовують API для доступу до журналів, метаданих і потоків подій у SaaS-сервісах. Це дозволяє аналізувати як контент переданих документів, так і контекст їхнього використання — авторів, одержувачів, час передачі, рівень доступу та можливість зовнішнього розшарування. У випадку виявлення порушення політики система може автоматично відключити зовнішній доступ, змінити права на документ, зашифрувати його або перемістити до захищеної директорії.

У межах архітектури важливим є модуль автентифікації та авторизації адміністративних користувачів. Оскільки адміністратори мають доступ до чутливих логів і політик, система повинна забезпечувати їхній захист за допомогою мультифакторної автентифікації, сегментації прав та детального аудиту. У великих компаніях адміністративні ролі зазвичай поділяються: одні відповідають за політики, інші — за аналіз інцидентів, треті — за технічну підтримку агентів. Це мінімізує ризик зловживання привілеями та підвищує прозорість роботи всієї інфраструктури DLP.

Окремим аспектом архітектури є модуль оптимізації продуктивності. Оскільки DLP може аналізувати великі обсяги трафіку та даних, необхідно забезпечити ефективну роботу системи без значного впливу на продуктивність

робочих станцій і серверів. Для цього використовуються механізми багаторівневого кешування, оптимізовані алгоритми пошуку шаблонів, апаратні прискорювачі шифрування, паралельна обробка даних і розвантаження частини завдань на хмарні сервіси. У деяких системах використовується адаптивне сканування — коли агент зменшує інтенсивність перевірки під час високого навантаження на ЦП або мережу, а потім повертається до нормального режиму після стабілізації системних ресурсів.

Ще одним важливим компонентом є механізм оновлення — політик, сигнатур, моделей ML, контентних шаблонів, класифікаторів та агентського програмного забезпечення. Система повинна забезпечувати централізоване керування оновленнями, можливість поетапного розгортання (наприклад, спочатку на тестову групу, потім на весь підрозділ) та перевірку сумісності з операційними системами та іншим корпоративним софтом. У хмарних DLP-рішеннях оновлення відбуваються автоматично, але для локальних інсталяцій адміністраторам необхідно планувати оновлення відповідно до внутрішніх процесів організації.

Архітектурно системи DLP повинні враховувати різноманітність операційних систем. Хоча Windows залишається основною платформою для корпоративних середовищ, дедалі частіше використовуються macOS та Linux. Кожна з них має свої механізми контролю ресурсів, тому агенти повинні бути адаптованими до специфічних API та драйверів. У деяких випадках агенти для Linux використовуються на серверах, де потрібно контролювати операції з файлами, базами даних або журнальними системами. Це забезпечує універсальність архітектури та дає змогу охопити всі потенційно ризикові точки.

Важливо, що архітектура DLP повинна забезпечувати безпеку самої системи від компрометації. Оскільки DLP працює з конфіденційними даними, її компоненти — політики, журнали, цифрові відбитки, аналітичні модулі — мають бути захищені від несанкціонованого доступу. Це реалізується за допомогою шифрування, сегментації адміністративних привілеїв, розмежування доступу до модулів, багаторівневої автентифікації та аудитних механізмів. У деяких системах

передбачено захист від деактивації агента: спроби вимкнути або видалити агент фіксуються як інцидент високого ризику.

Підсумовуючи, архітектура DLP є багаторівневою інтелектуальною системою, яка об'єднує мережеві, локальні, хмарні, аналітичні та поведінкові механізми в єдину платформу. Синергія між модулями забезпечує повний контроль над життєвим циклом даних: від їх створення до передачі, зберігання та видалення. Завдяки гнучкості, масштабованості та глибокій інтеграції з корпоративною інфраструктурою DLP стає ключовим елементом захисту інформаційних активів сучасних організацій, незалежно від їхнього розміру, структури чи галузевої специфіки. Архітектура DLP не є статичною — вона постійно розвивається разом із зростанням обсягу цифрових даних, появою нових каналів ексфільтрації, розширенням хмарних технологій та ускладненням бізнес-процесів. Саме тому DLP-рішення формують основу сучасної моделі Zero Trust та становлять критично важливий компонент екосистеми кібербезпеки.

2.3 Технології Data Classification у DLP системах

Класифікація даних є однією з ключових технологічних складових систем класу Data Loss Prevention, оскільки саме вона визначає, які інформаційні об'єкти підлягають захисту, яким чином і за яких умов мають застосовуватися політики контролю. У сучасних організаціях обсяги цифрової інформації зростають експоненційно, а дані циркулюють між різними інформаційними системами, користувачами, пристроями та хмарними сервісами. У таких умовах ручне визначення чутливості інформації стає неможливим, що зумовлює необхідність застосування автоматизованих технологій Data Classification, інтегрованих безпосередньо в DLP-рішення.

На відміну від класичних систем інформаційної безпеки, які зосереджуються на захисті інфраструктури або доступу до ресурсів, DLP-системи оперують даними як основним об'єктом контролю. Саме тому класифікація в межах DLP не є ізольованим процесом, а виступає динамічним механізмом, який тісно пов'язаний

із політиками доступу, каналами передачі інформації, контекстом дій користувача та рівнем ризику. Технології Data Classification дозволяють системі автоматично визначати, чи містить файл, текстовий фрагмент або потік даних конфіденційну інформацію, і відповідно ініціювати моніторинг, попередження або блокування дії.

У сучасних DLP-рішеннях класифікація даних реалізується як багаторівневий процес, що поєднує різні методи аналізу: структурний, контентний, контекстний, поведінковий та інтелектуальний. Такий підхід зумовлений необхідністю досягнення високої точності виявлення чутливих даних за одночасного зниження кількості хибнопозитивних спрацювань, які можуть негативно впливати на бізнес-процеси та продуктивність працівників.

Однією з базових технологій Data Classification у DLP-системах є класифікація на основі шаблонів та регулярних виразів. Цей метод ґрунтується на виявленні характерних структурних ознак даних, таких як формат номерів документів, банківських рахунків, ідентифікаційних кодів або персональних номерів.

Регулярні вирази дозволяють формально описати структуру таких даних і забезпечити швидке автоматизоване виявлення навіть у великих масивах текстової інформації. У практиці DLP цей підхід широко застосовується для захисту персональних даних, фінансової інформації та інших стандартизованих типів відомостей, що регулюються законодавством або внутрішніми політиками організації.

Разом із тим, виключно шаблонна класифікація має обмеження, оскільки вона не враховує контекст використання даних. Наприклад, числовий рядок, що формально відповідає шаблону банківського рахунку, може не мати жодного відношення до фінансової інформації в конкретному документі. Саме тому сучасні DLP-системи доповнюють регулярні вирази контентно-орієнтованим аналізом, який передбачає дослідження змісту документа або повідомлення з урахуванням ключових слів, тематичних ознак та семантичних зв'язків між елементами тексту. Контентний аналіз дозволяє значно підвищити точність класифікації, особливо у випадках роботи з неструктурованими даними.

Контентна класифікація в DLP-системах реалізується через механізми аналізу вмісту файлів різних форматів, зокрема текстових документів, електронних таблиць, презентацій, PDF-файлів, архівів та електронної пошти. Система виконує парсинг вмісту, нормалізацію тексту та застосовує відповідні правила класифікації незалежно від того, в якому форматі зберігається інформація. У випадку графічних файлів або сканованих документів використовуються технології оптичного розпізнавання символів, що дозволяє виявляти конфіденційні дані навіть у вигляді зображень. Це є важливим фактором, оскільки спроби обійти DLP шляхом перетворення тексту в зображення є поширеною тактикою витоку інформації.

Важливим елементом технологій Data Classification у DLP є контекстна класифікація, яка враховує не лише вміст даних, а й умови, за яких вони використовуються. Контекст може включати інформацію про користувача, його роль у системі, підрозділ, з якого виконується дія, застосунок, канал передачі, час доби, географічне розташування та інші фактори. Такий підхід дозволяє DLP-системам диференціювати допустимі та недопустимі дії з однаковими даними залежно від ситуації. Наприклад, передавання фінансового звіту між внутрішніми підрозділами може бути дозволеним, тоді як спроба копіювання того самого документа в особисту хмару користувача — заблокованою.

Окреме місце в технологіях класифікації даних займає метод цифрових відбитків документів (document fingerprinting). Цей підхід передбачає створення унікальних сигнатур на основі вмісту чутливих файлів або наборів даних, що дозволяє виявляти навіть частково змінені або фрагментовані копії документів.

Fingerprinting є особливо ефективним для захисту унікальних корпоративних матеріалів, таких як внутрішні звіти, договори, технічна документація або дослідницькі матеріали. На відміну від пошуку ключових слів, цифрові відбитки зберігають логічну структуру документа, що унеможливлює просте обходження захисту шляхом зміни формулювань або форматування.

У великих організаціях та фінансових установах широко застосовується технологія Exact Data Match, яка дозволяє зіставляти поточні дані з контрольними

наборами, наприклад, базами клієнтів або фінансовими реєстрами. Особливістю цього методу є використання хешованих або токенізованих представлень даних, що забезпечує високий рівень безпеки та відповідність вимогам захисту персональної інформації. Exact Data Match забезпечує надзвичайно високу точність класифікації, оскільки система порівнює дані з еталонним набором, а не покладається лише на формальні ознаки.

Суттєвим напрямом розвитку технологій Data Classification у DLP-системах є застосування лінгвістичних та семантичних методів аналізу. Такі методи дозволяють оцінювати зміст тексту з урахуванням мовних особливостей, контексту використання термінів та смислових зв'язків між словами. Семантична класифікація є особливо корисною для захисту інтелектуальної власності, внутрішньої переписки та аналітичних матеріалів, де чутлива інформація може передаватися у непрямій формі без використання очевидних шаблонів.

Останнім часом дедалі більшого поширення набувають алгоритми машинного навчання та штучного інтелекту, інтегровані в DLP-рішення для автоматичної класифікації даних. Такі алгоритми здатні навчатися на історичних даних, інцидентах безпеки та поведінкових моделях користувачів, поступово підвищуючи точність класифікації. Машинне навчання дозволяє виявляти нові типи чутливої інформації, адаптувати правила до специфіки конкретної організації та зменшувати кількість хибних спрацювань. У поєднанні з традиційними методами цей підхід формує гібридну модель класифікації, яка поєднує передбачуваність правил і адаптивність інтелектуальних алгоритмів.

Важливою особливістю сучасних технологій Data Classification у DLP є можливість динамічної класифікації, за якої рівень чутливості даних може змінюватися залежно від контексту їхнього використання. Наприклад, документ може не вважатися критичним під час внутрішнього редагування, але автоматично отримувати статус конфіденційного при спробі передачі за межі організації. Такий підхід дозволяє реалізувати гнучку модель захисту, що мінімізує втручання в бізнес-процеси та водночас забезпечує високий рівень безпеки.

Технології класифікації даних у DLP-системах тісно пов'язані з вимогами нормативно-правового регулювання та стандартами інформаційної безпеки. Автоматизована ідентифікація персональних даних, фінансової інформації та інших регульованих категорій дозволяє організаціям ефективніше виконувати вимоги таких нормативів, як GDPR, ISO/IEC 27001, PCI DSS та інших. Класифікація забезпечує прозорість обробки даних, спрощує аудит і знижує ризик порушень законодавства.

Таким чином, технології Data Classification у DLP-системах є центральним елементом, який забезпечує ефективність усієї системи захисту від витоку даних. Поєднання шаблонних, контентних, контекстних, поведінкових та інтелектуальних методів дозволяє DLP-рішенням адаптуватися до складних і динамічних корпоративних середовищ. Саме завдяки розвинутим технологіям класифікації DLP-системи здатні забезпечити комплексний контроль над інформаційними потоками та виступати ключовим інструментом захисту даних у сучасних організаціях.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ДАНИХ НА ОСНОВІ DLP РІШЕННЯ

3.1 Проектування архітектури впровадження DLP-системи ManageEngine в організації

Проектування архітектури впровадження DLP-системи є критично важливим етапом побудови ефективного механізму захисту інформації в організації, оскільки саме на цьому етапі визначаються принципи розміщення компонентів, їх взаємодія, масштаби контролю даних та інтеграція з наявною IT-інфраструктурою. У випадку використання ManageEngine Endpoint DLP архітектурне проектування повинно враховувати особливості даного рішення, його агентську модель, централізований підхід до керування політиками, а також вимоги до контролю даних у станах використання, передачі та зберігання.

Сучасне корпоративне середовище характеризується гібридною структурою, у межах якої поєднуються локальні робочі станції, серверна інфраструктура, віддалені робочі місця, мобільні пристрої та хмарні сервіси. У таких умовах архітектура DLP-системи має бути масштабованою, стійкою до збоїв та здатною забезпечувати безперервний контроль даних незалежно від фізичного розташування користувача. ManageEngine Endpoint DLP реалізує централізовану модель управління з використанням керуючого сервера та агентів кінцевих точок, що дозволяє забезпечити єдину політику безпеки в межах усієї організації.

Базовим елементом архітектури впровадження ManageEngine Endpoint DLP є центральний сервер керування, який виконує функції зберігання політик, конфігурацій, правил класифікації, журналів подій та інцидентів безпеки. Даний сервер, як правило, розгортається у внутрішній мережі організації або в

захищеному сегменті дата-центру, що забезпечує контроль доступу та відповідність вимогам інформаційної безпеки. Центральний сервер є логічним ядром системи, через яке здійснюється адміністрування, аналіз інцидентів, формування звітності та кореляція подій.

Архітектура впровадження передбачає інтеграцію сервера ManageEngine DLP з наявною інфраструктурою управління ідентифікацією та доступом. Зокрема, взаємодія з корпоративним каталогом (Active Directory) дозволяє застосовувати політики DLP з урахуванням організаційної структури, ролей користувачів та груп безпеки. Такий підхід забезпечує контекстно-залежний контроль, коли однакові дані можуть оброблятися по-різному залежно від підрозділу, посади або рівня доступу користувача.

Другим ключовим компонентом архітектури є агенти ManageEngine Endpoint DLP, які встановлюються на робочі станції та сервери кінцевих користувачів. Саме агентська модель забезпечує глибокий контроль даних у стані використання, що є однією з основних переваг ManageEngine Endpoint DLP. Агенти працюють на рівні операційної системи, перехоплюючи дії користувача, пов'язані з обробкою файлів, буфером обміну, друком, екранним захопленням, використанням змінних носіїв та передаванням інформації через веб-канали або електронну пошту.

Під час проєктування архітектури важливо визначити масштаб агентського покриття. У типовому корпоративному сценарії агенти встановлюються на всі робочі станції співробітників, які мають доступ до конфіденційної інформації, а також на сервери, що виконують роль файлових сховищ або обробляють критичні дані. При цьому архітектура повинна враховувати продуктивність агентів, щоб контроль не впливав негативно на роботу користувачів. ManageEngine Endpoint DLP використовує локальні кеші політик та оптимізовані механізми аналізу, що дозволяє мінімізувати затримки та навантаження на систему.

Окрему увагу в архітектурі впровадження слід приділити мережевій взаємодії між агентами та сервером керування. Комунікація здійснюється захищеними каналами з використанням криптографічних механізмів, що

унеможливлує перехоплення або модифікацію переданих даних. Агенти передають на сервер інформацію про події, інциденти та журнали дій користувачів, а сервер, у свою чергу, розповсюджує оновлення політик і правил класифікації. У разі тимчасової відсутності мережевого з'єднання агенти продовжують працювати автономно, використовуючи локально збережені політики, а після відновлення зв'язку виконують синхронізацію.

Архітектура впровадження ManageEngine Endpoint DLP також передбачає розмежування режимів роботи системи залежно від етапу її впровадження. На початковому етапі зазвичай використовується режим моніторингу (audit mode), який дозволяє зібрати статистику щодо руху даних та потенційних ризиків без блокування дій користувачів. Це дає змогу адаптувати політики до реальних бізнес-процесів організації та зменшити ймовірність хибнопозитивних спрацювань. Після етапу аналізу архітектура переходить у режим активного захисту, коли критичні дії з даними блокуються або потребують підтвердження.

Важливою складовою архітектури є механізми класифікації даних, інтегровані безпосередньо в Endpoint DLP. У процесі проєктування визначаються категорії чутливих даних, методи їх виявлення та правила обробки. ManageEngine Endpoint DLP підтримує класифікацію на основі регулярних виразів, ключових слів, контентного аналізу та контекстних атрибутів. Це дозволяє реалізувати гнучку модель контролю, коли архітектура DLP адаптується до специфіки інформаційних потоків організації.

Архітектура впровадження також повинна враховувати інтеграцію з іншими системами інформаційної безпеки. Хоча ManageEngine Endpoint DLP є автономним рішенням, можливість експорту журналів та інцидентів у зовнішні системи аналізу дозволяє розширити функціональність захисту. У корпоративному середовищі це може бути використано для централізованого аудиту, внутрішніх розслідувань та забезпечення відповідності нормативним вимогам.

З точки зору безперервності бізнесу архітектура DLP-системи повинна бути стійкою до відмов окремих компонентів. Проєктування може передбачати

резервне копіювання конфігурацій, журналів та політик, а також можливість швидкого відновлення сервера керування. Хоча ManageEngine Endpoint DLP зазвичай розгортається як єдиний керуючий вузол, його архітектура дозволяє мінімізувати ризики, пов'язані з тимчасовою недоступністю сервера, завдяки автономній роботі агентів.

Таким чином, проєктування архітектури впровадження DLP-системи ManageEngine в організації базується на принципах централізованого управління, агентського контролю кінцевих точок, контекстної класифікації даних та гнучкої інтеграції з корпоративною інфраструктурою. Така архітектура забезпечує комплексний захист інформаційних активів, дозволяє адаптувати політики безпеки до реальних бізнес-процесів і створює основу для подальшого розгортання практичних механізмів контролю та запобігання витокам даних, що розглядатимуться у наступних підрозділах роботи.

3.2 Налаштування політик контролю даних та класифікації у ManageEngine Endpoint DLP

Практична реалізація політик контролю даних у середовищі ManageEngine Endpoint DLP базується на поєднанні двох ключових механізмів: класифікації конфіденційної інформації та примусового контролю каналів її використання і передачі. На відміну від концептуального рівня, розглянутого в попередніх розділах, у даному підпункті акцент зроблено саме на технічних аспектах налаштування політик, їхній взаємодії з агентами кінцевих точок та практичній перевірці ефективності впроваджених правил.

Першим етапом налаштування DLP у ManageEngine є розгортання агентської інфраструктури, оскільки саме агент кінцевої точки виконує контроль дій користувача в режимі реального часу. На скріншоті з інтерфейсу керування агентами видно, що агент успішно встановлений на робочій станції, має актуальний статус підключення та регулярно передає телеметрію до центрального сервера керування. Наявність активного агента є обов'язковою умовою для

роботи таких механізмів, як контроль доступу до файлів, блокування буфера обміну, аналіз друку, моніторинг веб-завантажень і взаємодія з локальними додатками. Саме на цьому рівні формується точка примусового виконання політик DLP.

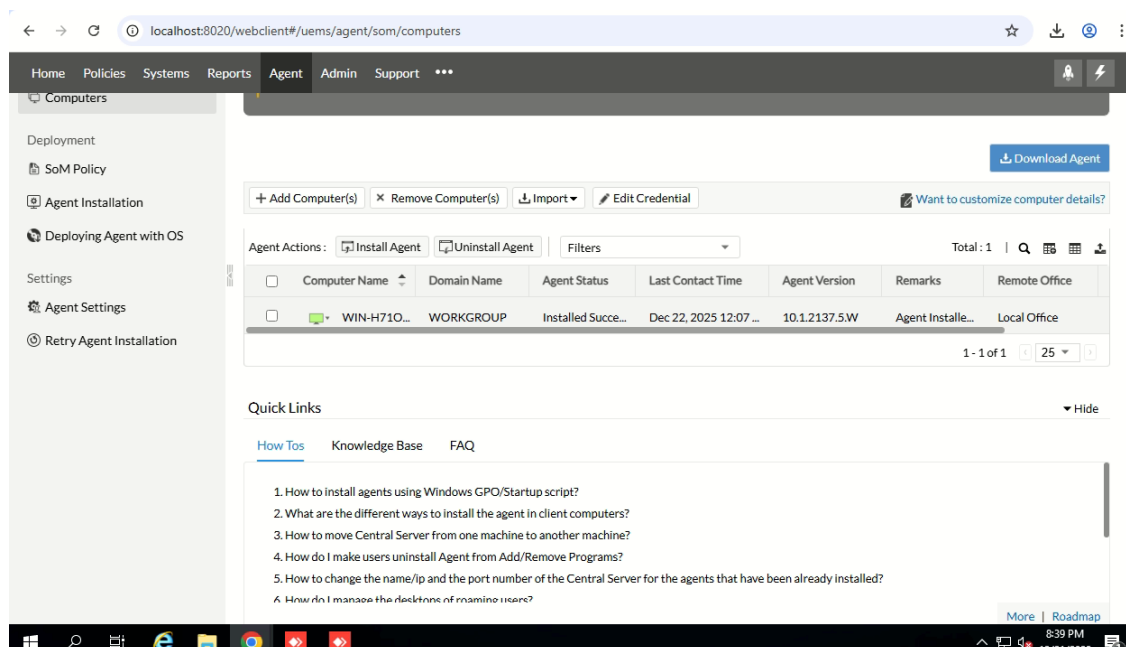


Рис. 3.1. Встановлений Агент

Після підтвердження коректної роботи агентів здійснюється створення правил класифікації даних (Data Rules), які визначають, який саме контент вважається чутливим. У практичному прикладі використовується правило класифікації банківської інформації, зокрема номерів IBAN. У вікні налаштування правила застосовано декілька регулярних виразів, що дозволяє виявляти як самі значення IBAN, так і контекстні згадки, пов'язані з банківськими реквізитами. Такий підхід значно знижує ймовірність хибних спрацювань і водночас підвищує точність детекції, оскільки система аналізує не лише формат даних, а й їхнє семантичне оточення.

Використання кількох regex-патернів в межах одного правила демонструє практичну реалізацію комбінованої класифікації, коли рішення про чутливість даних ухвалюється на основі сукупності ознак. Це особливо важливо для фінансової інформації, яка може зберігатися у різних форматах і використовуватися в різних бізнес-процесах.

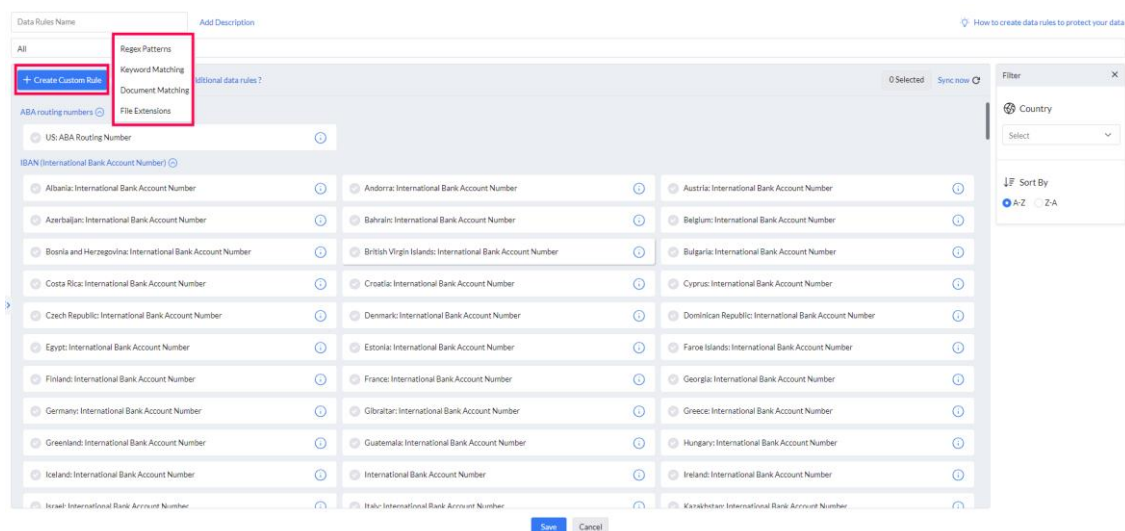


Рис 3.2.2. Створення правил

Наступним кроком є прив'язка створених правил класифікації до політик Data Loss Prevention, які визначають, яким чином система повинна реагувати на виявлення чутливого контенту. У політиці DLP конфігуруються окремі канали контролю, кожен з яких відповідає за конкретний сценарій витоку інформації. Серед таких каналів — доступ до файлів, завантаження через веб-браузери, передавання через електронну пошту, друк, робота зі змінними носіями та взаємодія з локальними і віддаленими застосунками.

На скріншоті з налаштування політики видно, що для більшості критичних каналів обрано режим блокування у разі виявлення чутливих даних. Наприклад, завантаження файлів через браузери обмежується лише дозволеними сценаріями, а передавання конфіденційної інформації через електронну пошту блокується автоматично. Водночас для деяких дій, таких як знімки екрана, на початковому етапі може використовуватися дозволяючий або аудиторський режим з метою аналізу поведінки користувачів і зниження ризику порушення бізнес-процесів.

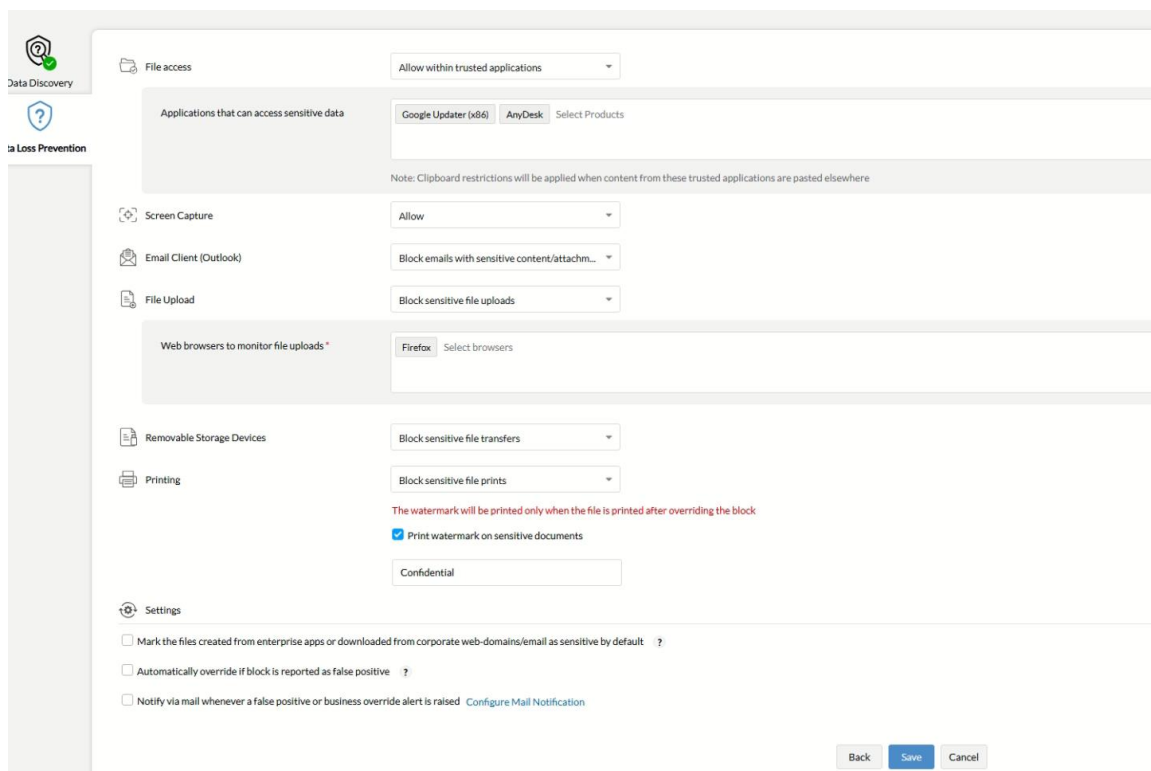


Рис. 3.2. Налаштування Політик

Окремої уваги заслуговує механізм контролю доступу до файлів у контексті довірених застосунків. У політиці передбачена можливість визначення списку програм, яким дозволено працювати з чутливими даними без негайного блокування. На практиці це використовується для корпоративних інструментів, таких як внутрішні оновлювачі, службові утиліти або віддалені засоби адміністрування. Водночас система чітко зазначає, що обмеження буфера обміну застосовуватимуться у разі спроби вставлення чутливого контенту з таких застосунків у сторонні або недовірені середовища. Таким чином реалізується принцип контекстного контролю, коли дозволені дії в межах одного застосунку можуть бути заблоковані при зміні контексту використання даних.

Важливим елементом практичної конфігурації є контроль друку чутливих документів. Політика дозволяє не лише блокувати спроби друку, а й застосовувати водяні знаки у випадках, коли друк дозволено після явного підтвердження. Це забезпечує додатковий рівень стримування та підзвітності, оскільки кожен надрукований документ містить маркування з рівнем конфіденційності та може бути пов'язаний із конкретним користувачем.

Окремим технічним аспектом, який підтверджується експериментальними тестами, є розмежування етапів виявлення та блокування. У процесі тестування було встановлено, що контент може бути коректно виявлений механізмами класифікації (regex-аналіз, контекстні правила), однак дія користувача не буде заблокована, якщо відповідний канал не має активного примусового правила. Це демонструє багаторівневу архітектуру ManageEngine Endpoint DLP, де механізми детекції та механізми реагування функціонують незалежно й потребують окремого налаштування для кожного каналу витоку.

Практичні тести з використанням файлів, що містять IBAN-дані, підтвердили, що при правильному поєднанні Data Rule та DLP-політики система здатна не лише фіксувати інцидент, а й ефективно блокувати небажані дії, такі як передавання файлів через веб-інтерфейси або спроби відкриття документів без належних прав доступу. Повідомлення операційної системи про відсутність дозволу на доступ до файлу свідчить про те, що блокування відбувається на рівні агента, ще до завершення операції користувача.

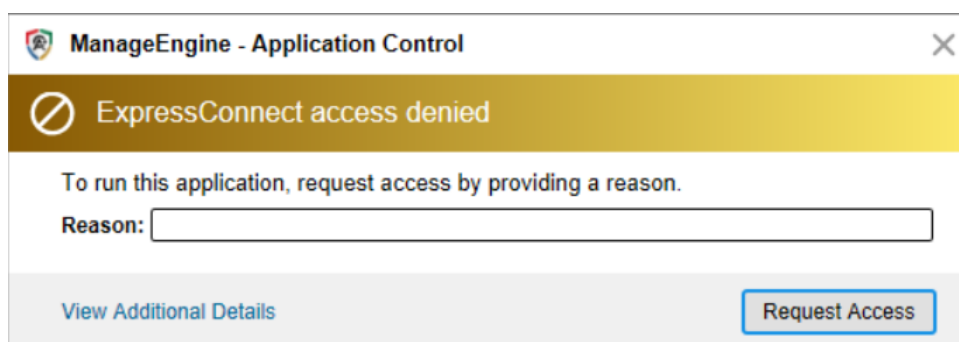


Рис. 3.3. Блокування підозрілої дії

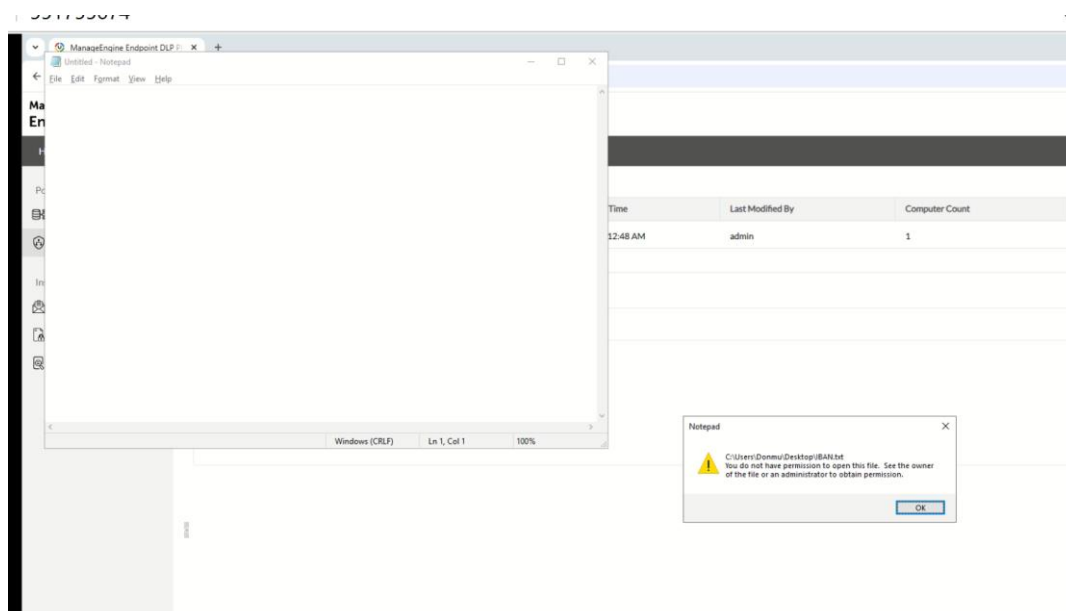


Рис. 3.4. Блокування підозрілої дії

З технічної точки зору важливою є також пріоритетність політик. У ManageEngine Endpoint DLP політики застосовуються відповідно до заданих умов і порядку, що дозволяє уникнути конфліктів між дозволяючими та забороняючими правилами. У межах практичного впровадження це дає змогу, наприклад, дозволити доступ до чутливих даних у межах внутрішніх бізнес-процесів, але жорстко блокувати будь-які спроби їх ексфільтрації за межі корпоративного середовища.

Таким чином, налаштування політик контролю даних та класифікації у ManageEngine Endpoint DLP являє собою комплексний процес, що включає розгортання агентів, створення точних правил класифікації, конфігурацію каналів контролю та перевірку ефективності примусового виконання політик. Практична реалізація, підтверджена наведеними скріншотами, демонструє, що система здатна забезпечити гнучкий, контекстно-орієнтований та масштабований захист конфіденційної інформації, що відповідає сучасним вимогам до інформаційної безпеки корпоративних середовищ.

У межах дослідження було встановлено, що дефолтні регулярні вирази ManageEngine Endpoint DLP у багатьох випадках спрацьовують лише на рівні контентного сканування (Data Discovery), однак не ініціюють примусові дії блокування (Data Loss Prevention Enforcement). Це пов'язано з тим, що Policy

Engine системи не розглядає такі спрацювання як події з достатнім рівнем впевненості (confidence level), необхідним для застосування обмежень до дій користувача. Як наслідок, навіть за наявності виявлених банківських реквізитів операції копіювання, вставлення або передавання даних можуть бути дозволені.

Для вирішення зазначеної проблеми в роботі запропоновано використання кастомного контекстно-орієнтованого регулярного виразу, який поєднує структурну перевірку фінансових реквізитів із семантичним аналізом текстового оточення. Такий підхід ґрунтується на припущенні, що у реальних бізнес-сценаріях банківські дані майже завжди супроводжуються характерними ключовими словами, що вказують на їхню семантичну природу (наприклад, “IBAN”, “Bank”, “Account”, “Konto”, “Kontonummer”, “Bankverbindung” тощо).

Запропонований регулярний вираз має вигляд:

```
(?i)\b(
iban|
bic|
swift|
bank|
account|
konto|
kontonummer|
bankverbindung|
routing\s*number|
sort\s*code|
account\s*number|
card\s*number|
credit\s*card|
debit\s*card
)\b[[:s:]]*[A-Z]{2}\d{2}[A-Z0-9]{11,30}\b\d{8,20}\b
```

Даний шаблон реалізує багаторівневу модель класифікації, у межах якої одночасно перевіряється:

1. Наявність семантичного контексту — ключових слів, що характерні для фінансової документації та банківських операцій.
2. Структурна валідність даних — відповідність формату міжнародного банківського рахунку або номеру рахунку загальноприйнятим стандартам.
3. Незалежність від способу передачі — можливість виявлення даних як у файлах, так і під час операцій Data-in-Use (Clipboard, вставлення у форми, месенджери або браузері).

Порівняльний аналіз показав, що запропонований контекстно-структурний регулярний вираз значно знижує кількість хибнонегативних спрацьовувань (false negatives) у порівнянні зі стандартними шаблонами. Крім того, завдяки підвищеному рівню впевненості у визначенні типу даних, Policy Enforcement Engine ManageEngine Endpoint DLP коректно інтерпретує такі події як критичні та застосовує примусові політики, зокрема блокування копіювання до буфера обміну, заборону завантаження файлів у веббраузерах та блокування передавання через електронну пошту.

Особливо важливим є той факт, що запропонований підхід демонструє високу ефективність саме у сценаріях Data-in-Use, які є найбільш складними для контролю в DLP-системах. На відміну від аналізу даних у стані спокою (Data-at-Rest), контроль операцій користувача в реальному часі потребує мінімізації затримок та максимальної точності прийняття рішень. Контекстно-орієнтований регулярний вираз дозволяє досягти балансу між продуктивністю та точністю, оскільки зменшує кількість хибнопозитивних спрацьовувань і водночас забезпечує надійне виявлення дійсно чутливої інформації.

З точки зору наукової новизни, запропонований підхід відрізняється від традиційних методів класифікації даних у DLP-системах тим, що поєднує синтаксичний аналіз із елементами семантичного розпізнавання. Таким чином, класифікація базується не лише на формі даних, а й на змісті та контексті їх використання, що відповідає сучасним тенденціям розвитку інтелектуальних систем захисту інформації.

У практичному аспекті використання кастомного контекстно-орієнтованого

регулярного виразу дозволяє підвищити ефективність політик запобігання витоку банківських даних без необхідності значного ускладнення архітектури системи або впровадження додаткових зовнішніх модулів. Запропоноване рішення легко інтегрується у наявні механізми ManageEngine Endpoint DLP та може бути адаптоване до специфіки конкретної організації шляхом розширення набору ключових слів або уточнення структурних шаблонів.

Отже, застосування контекстно-структурних регулярних виразів є доцільним та обґрунтованим підходом до підвищення точності класифікації банківських даних у DLP-системах і дозволяє забезпечити більш надійний захист фінансової інформації в умовах сучасних корпоративних середовищ.

3.3 Контроль каналів передачі даних та моніторинг інцидентів витоку в ManageEngine Endpoint DLP

Одним із ключових завдань систем класу Data Loss Prevention є забезпечення контролю над каналами передачі інформації та своєчасне виявлення інцидентів витоку даних у корпоративному середовищі. На відміну від традиційних засобів інформаційної безпеки, які переважно фокусуються на мережевому периметрі або захисті інфраструктури, DLP-системи орієнтовані на захист самих даних незалежно від того, яким шляхом вони передаються або яким чином використовуються. У цьому контексті ManageEngine Endpoint DLP реалізує комплексний підхід до контролю каналів передачі інформації, поєднуючи технічні механізми блокування, детальний моніторинг дій користувачів та централізовану систему обробки інцидентів.

У сучасних організаціях канали потенційного витоку даних є надзвичайно різноманітними. Окрім класичних каналів, таких як електронна пошта або знімні носії, дедалі більшого значення набувають веббраузери, хмарні сервіси, буфер обміну (Clipboard), інструменти віддаленого доступу, корпоративні та зовнішні месенджери, а також механізми друку та створення знімків екрана. ManageEngine Endpoint DLP враховує цю багатоканальність і надає можливість централізовано

контролювати всі основні вектори ексфільтрації даних на рівні кінцевих точок.

Контроль передачі даних у ManageEngine Endpoint DLP реалізується через політики Data Loss Prevention, які застосовуються до визначених груп пристроїв, користувачів або організаційних підрозділів. Кожна політика містить набір правил, що визначають дозволені, обмежені або заборонені дії з чутливою інформацією залежно від її класифікації. Важливою особливістю є те, що рішення працює не лише з файлами як об'єктами, а й з операціями користувача, що дозволяє контролювати дані у стані використання (Data-in-Use).

Одним із найбільш критичних каналів передачі даних у сучасному корпоративному середовищі є буфер обміну. Саме через Clipboard часто відбувається несанкціоноване копіювання фрагментів конфіденційної інформації з внутрішніх систем у зовнішні застосунки, вебформи або месенджери. ManageEngine Endpoint DLP забезпечує контроль операцій копіювання та вставлення шляхом перехоплення відповідних системних викликів на рівні операційної системи. У разі виявлення чутливого контенту, що відповідає правилам класифікації, система може заблокувати операцію, замінити вміст буфера обміну, зафіксувати інцидент або дозволити дію з попередженням користувача, залежно від налаштувань політики.

Не менш важливим каналом є передавання даних через веббраузери. З огляду на активне використання хмарних сервісів, файлообмінників та вебдодатків, контроль вебзавантажень стає критично необхідним. ManageEngine Endpoint DLP дозволяє визначати конкретні браузери, для яких застосовується контроль завантаження файлів, а також блокувати або дозволяти передавання даних залежно від типу контенту та рівня його конфіденційності. Такий підхід забезпечує баланс між безпекою та зручністю роботи користувачів, дозволяючи, наприклад, обмежити передавання фінансових або персональних даних, не блокуючи при цьому легітимні бізнес-процеси.

Контроль електронної пошти є ще одним важливим елементом захисту від витоку інформації. У ManageEngine Endpoint DLP реалізовано механізми інтеграції з поштовими клієнтами, зокрема Microsoft Outlook, що дозволяє аналізувати вміст

листів та вкладень перед їх відправленням. У разі виявлення чутливої інформації система може автоматично заблокувати надсилання повідомлення, видалити вкладення, застосувати водяний знак або зафіксувати інцидент для подальшого розслідування. Такий підхід особливо ефективний для запобігання випадковим витокам, які часто виникають унаслідок людського фактору.

Знімні носії інформації традиційно залишаються одним із найбільш ризикових каналів витоку даних. ManageEngine Endpoint DLP надає можливість контролювати підключення USB-накопичувачів та інших зовнішніх пристроїв, а також обмежувати операції копіювання на них чутливих файлів. Політики можуть бути налаштовані таким чином, щоб повністю блокувати передавання конфіденційних даних на знімні носії або дозволяти такі операції лише для авторизованих пристроїв чи користувачів. Усі дії при цьому фіксуються в системі моніторингу інцидентів.

Окрему увагу в ManageEngine Endpoint DLP приділено контролю операцій друку. Друк документів, що містять конфіденційну інформацію, може становити серйозну загрозу безпеці, особливо у великих організаціях із відкритими офісними просторами. Система дозволяє блокувати друк чутливих файлів або застосовувати до них водяні знаки, які містять ідентифікаційну інформацію користувача, дату та час друку. Це не лише зменшує ризик навмисного витоку, а й підвищує рівень відповідальності персоналу.

Контроль створення знімків екрана та використання інструментів захоплення зображень також є важливим аспектом захисту інформації. У ManageEngine Endpoint DLP передбачено можливість обмежувати або забороняти знімання екрана в застосунках, що працюють із чутливими даними. Такий механізм особливо актуальний для фінансових систем, CRM, ERP та інших корпоративних платформ, де інформація відображається на екрані, але не завжди зберігається у вигляді файлів.

Ефективність контролю каналів передачі даних значною мірою залежить від системи моніторингу інцидентів витоку інформації. ManageEngine Endpoint DLP реалізує централізований механізм збору, обробки та аналізу подій безпеки, що

виникають у процесі роботи користувачів. Кожна спроба порушення політики фіксується як інцидент, який містить детальну інформацію про користувача, пристрій, тип даних, канал передачі, час події та прийняте рішення.

Моніторинг інцидентів здійснюється через аналітичні панелі та журнали, що дозволяють фахівцям з інформаційної безпеки оперативно оцінювати поточний стан захищеності даних. Система підтримує фільтрацію, пошук та агрегацію інцидентів за різними параметрами, що спрощує аналіз великих обсягів подій у масштабних корпоративних середовищах. Окрім цього, ManageEngine Endpoint DLP дозволяє визначати рівень критичності інцидентів, що дає змогу пріоритизувати реагування на найбільш небезпечні порушення.

Важливою складовою моніторингу є можливість контекстного аналізу інцидентів. Система враховує не лише сам факт передачі даних, а й умови, за яких вона відбулася: тип користувача, час доби, застосунок-джерело, попередню активність, а також історію подібних дій. Такий підхід дозволяє відрізнити навмисні спроби витоку від легітимних бізнес-операцій, що зменшує кількість хибнопозитивних спрацювань і підвищує ефективність роботи служби безпеки.

ManageEngine Endpoint DLP також підтримує механізми сповіщення та автоматизованого реагування на інциденти. У разі виявлення критичного порушення система може надсилати повідомлення відповідальним особам, створювати записи у системах управління інцидентами або ініціювати додаткові заходи захисту, такі як посилений моніторинг користувача або тимчасове обмеження доступу. Це дозволяє скоротити час реагування та мінімізувати потенційні наслідки витоку даних.

Значну роль у моніторингу інцидентів відіграє журналювання подій. ManageEngine Endpoint DLP зберігає детальні журнали, які можуть бути використані для подальшого аналізу, аудиту або цифрової експертизи. Наявність повного ланцюжка подій — від виявлення чутливого контенту до застосування політики — є важливою умовою відповідності нормативним вимогам та внутрішнім стандартам інформаційної безпеки.

Таким чином, контроль каналів передачі даних у ManageEngine Endpoint DLP

реалізується як багаторівнева система, що охоплює всі основні вектори витоку інформації на рівні кінцевих точок. Поєднання примусових політик, контекстного аналізу та розвинених механізмів моніторингу інцидентів дозволяє не лише запобігати витокам даних, а й забезпечувати прозорість, керованість та доказову базу для подальшого реагування. Це робить ManageEngine Endpoint DLP ефективним інструментом захисту інформаційних активів організації в умовах сучасних гібридних та розподілених робочих середовищ.

3.4 Рекомендації щодо впровадження, оптимізації та експлуатації DLP-системи в організації

На основі проведеного аналізу проблеми витоку даних, дослідження сучасних підходів до захисту інформації, вивчення архітектури DLP-систем та практичного налаштування ManageEngine Endpoint DLP, можна сформувати комплекс рекомендацій, спрямованих на ефективне впровадження, подальшу оптимізацію та безпечну експлуатацію DLP-рішень у корпоративному середовищі.

Першочерговим етапом впровадження DLP має бути формування чіткого розуміння цінності інформаційних активів організації. До початку технічного розгортання необхідно провести інвентаризацію даних, визначити типи інформації, що підлягають захисту, та їхню критичність для бізнес-процесів. Особливу увагу слід приділяти персональним даним, фінансовій інформації, комерційній таємниці, внутрішній технічній документації та даним клієнтів. Без цього етапу впровадження DLP ризикує перетворитися на формальний контроль без реального зниження ризиків.

Рекомендується починати впровадження DLP із режиму моніторингу (audit mode), не застосовуючи негайне блокування дій користувачів. Такий підхід дозволяє зібрати статистику реальних потоків даних, визначити типові сценарії використання інформації та виявити потенційно ризикові дії без негативного впливу на бізнес-процеси. На основі зібраних журналів можна поступово формувати політики контролю, адаптовані до специфіки організації.

Архітектура впровадження повинна бути гібридною та поетапною. Доцільно

розгортати DLP-агенти спочатку на тестовій групі користувачів або окремому підрозділі, що дозволяє перевірити сумісність із прикладним програмним забезпеченням, оцінити вплив на продуктивність робочих станцій та скоригувати політики до масового розгортання. Особливо важливо протестувати роботу агентів у сценаріях віддаленого доступу, використання VPN та роботи з хмарними сервісами.

Політики DLP повинні будуватися не лише на принципі заборони, а й на основі контекстного та ризик-орієнтованого підходу. Рекомендується використовувати багаторівневу класифікацію даних, поєднуючи автоматичні методи (regex, шаблони, машинне навчання) з ручним маркуванням критично важливих документів. Такий підхід знижує залежність від людського фактору та підвищує точність виявлення конфіденційної інформації.

Особливу увагу слід приділяти контролю каналів передачі даних, які найчастіше використовуються для несанкціонованих витоків: буфер обміну, веббраузери, хмарні сховища, зовнішні носії та електронна пошта. Політики для цих каналів повинні враховувати не лише тип даних, але й контекст дії: роль користувача, пристрій, час виконання операції та тип каналу. Наприклад, передавання конфіденційного документа всередині корпоративної мережі може бути дозволеним, тоді як аналогічна дія через публічний хмарний сервіс — заблокованою.

Рекомендується активно використовувати власні регулярні вирази та кастомні правила класифікації, адаптовані до локальних форматів даних, мови документів та бізнес-специфіки організації. Це дозволяє підвищити ефективність DLP у порівнянні з використанням стандартних шаблонів, які часто не враховують регіональні або галузеві особливості.

Після початкового впровадження DLP-системи важливим завданням є постійна оптимізація політик та зменшення кількості хибнопозитивних спрацьовувань. Надмірна кількість блокувань або попереджень негативно впливає на продуктивність працівників та може призвести до ігнорування повідомлень системи. Рекомендується регулярно аналізувати журнали інцидентів, коригувати

правила та додавати обґрунтовані винятки для легітимних бізнес-сценаріїв.

Доцільно впроваджувати ризик-орієнтовану модель контролю, за якої рівень обмежень залежить від поведінки користувача. Працівники з підвищеним ризиковим профілем можуть підлягати жорсткішому контролю, тоді як для інших користувачів застосовуються більш гнучкі правила. Такий підхід дозволяє оптимізувати навантаження на систему та зосередити ресурси безпеки на найбільш критичних ділянках.

Оптимізація продуктивності також передбачає правильне налаштування сканування даних у стані спокою. Рекомендується використовувати інкрементальне сканування та планувати ресурсоємні перевірки поза піковими годинами роботи. Це знижує навантаження на файлові сервери та мережеву інфраструктуру без зменшення рівня безпеки.

Ефективна експлуатація DLP неможлива без належної організації процесів управління інцидентами. Рекомендується визначити відповідальних осіб або команду, яка здійснює аналіз спрацювань, реагування на інциденти та комунікацію з бізнес-підрозділами. Інтеграція DLP із SIEM та SOAR-системами дозволяє автоматизувати частину реагування та скоротити час виявлення і нейтралізації загроз.

Важливим аспектом експлуатації є регулярне навчання персоналу. DLP не повинна сприйматися як каральний інструмент, а як засіб підтримки безпечної роботи з даними. Інформування користувачів про причини блокувань, правила обробки інформації та потенційні ризики сприяє формуванню культури інформаційної безпеки та зменшенню кількості інцидентів, пов'язаних із людським фактором.

Рекомендується також забезпечити регулярний аудит налаштувань DLP-системи. Зміни у бізнес-процесах, організаційній структурі або IT-інфраструктурі повинні супроводжуватися переглядом політик контролю даних. Це особливо актуально в умовах цифрової трансформації, активного використання хмарних сервісів та віддаленої роботи.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження проблеми захисту конфіденційних даних та запобігання їх витоку в сучасних організаціях. Визначено актуальність теми, сформульовано мету, об'єкт, предмет та основні завдання дослідження, що відповідають сучасним викликам у сфері кібербезпеки та вимогам до захисту інформаційних ресурсів.

У першому розділі роботи досліджено сутність проблеми витоку даних в організації, проаналізовано основні загрози інформаційній безпеці, зокрема внутрішні інсайдерські ризики, людський фактор, неконтрольоване використання цифрових каналів передачі даних та зростання ролі хмарних сервісів. Проведено аналіз підходів до захисту даних від витоку та обґрунтовано центральну роль DLP-рішень у сучасних системах захисту інформації. Розглянуто існуючі класи рішень для запобігання витокам даних і визначено, що саме DLP-системи забезпечують контентно та контекстно орієнтований контроль над інформаційними потоками незалежно від каналу або середовища їх використання.

У другому розділі виконано аналіз методів і засобів захисту даних на базі сучасних DLP-рішень. Визначено призначення та основні функції DLP-систем, зокрема контроль даних у станах використання, передачі та зберігання, класифікацію інформації, примусове виконання політик безпеки, моніторинг дій користувачів та реагування на інциденти. Досліджено загальну архітектуру DLP-систем, її основні компоненти та принципи побудови, що дозволяють забезпечити масштабованість, гнучкість і стійкість до відмов у гібридних корпоративних середовищах.

Окрему увагу приділено технологіям класифікації даних у DLP-системах. Розглянуто синтаксичні, контекстні та семантичні методи класифікації, а також їх поєднання в межах сучасних інтелектуальних DLP-рішень. У роботі обґрунтовано доцільність використання комбінованого підходу до класифікації даних, який поєднує регулярні вирази, контентний аналіз і контекстні ознаки, що дозволяє зменшити кількість хибнопозитивних спрацьовувань та підвищити точність виявлення конфіденційної інформації.

У третьому розділі розроблено технологію захисту даних в організації на основі DLP-системи ManageEngine Endpoint DLP. Проведено проєктування архітектури впровадження рішення в корпоративному середовищі з урахуванням агентської моделі, централізованого управління політиками та особливостей гібридної інфраструктури. Показано, що запропонована архітектура забезпечує ефективний контроль даних незалежно від фізичного розташування користувачів і типу використовуваних каналів передачі інформації.

Практична частина роботи присвячена налаштуванню політик контролю даних та класифікації у ManageEngine Endpoint DLP. Реалізовано та перевірено політики контролю буфера обміну, веб-завантажень, доступу до файлів і передачі даних, що дозволило продемонструвати ефективність блокування несанкціонованих дій на рівні кінцевих точок. Запропоновано та апробовано контекстно-структурний регулярний вираз для виявлення банківських даних, який поєднує синтаксичний аналіз із семантичним контекстом. Застосування такого підходу дозволяє підвищити точність класифікації фінансової інформації та підтверджує наукову новизну отриманих результатів.

Також у роботі досліджено механізми контролю каналів передачі даних і моніторингу інцидентів витоку в ManageEngine Endpoint DLP. Показано, що система забезпечує централізований збір журналів, детальну фіксацію дій користувачів, кореляцію подій та можливість інтеграції з іншими засобами інформаційної безпеки. Це дозволяє своєчасно виявляти порушення політик, аналізувати їх причини та забезпечувати ефективне реагування на інциденти.

На основі результатів дослідження розроблено рекомендації щодо впровадження, оптимізації та експлуатації DLP-системи в організації. Запропоновано поетапний підхід до розгортання DLP, використання режиму моніторингу на початковому етапі, регулярний аналіз журналів і коригування політик з урахуванням реальних бізнес-процесів. Обґрунтовано доцільність інтеграції DLP у загальну екосистему кібербезпеки організації та застосування ризик-орієнтованої моделі контролю даних.

Таким чином, у роботі досягнуто поставленої мети та вирішено основні

завдання дослідження. Запропонована технологія захисту даних на основі DLP-системи ManageEngine Endpoint DLP є науково обґрунтованою та практично значущою і може бути використана для підвищення рівня захисту інформаційних ресурсів організацій різного масштабу та сфери діяльності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Eric Ouellet. Data Loss Prevention For Dummies. Forcepoint Special Edition. John Wiley & Sons, Inc. 2022.

URL: <https://www.forcepoint.com/sites/default/files/resources/files/data-loss-prevention-for-dummies.pdf>

(дата звернення: 22.10.2025).

2. 2023 Cost of Insider Threats Global Report. Ponemon Institute.

URL: <https://www.ponemon.org/library/cost-of-insider-threats>

(дата звернення: 22.10.2025).

3. 2023 Data Breach Investigations Report. Verizon.

URL: <https://www.verizon.com/business/resources/reports/dbir/>

(дата звернення: 22.10.2025).

4. Rich Mogull, Adrian Lane. Understanding and Selecting Data Loss Prevention. Securosis Research. 2021.

URL: <https://securosis.com/research/understanding-and-selecting-dlp>

(дата звернення: 22.10.2025).

5. Neil MacDonald, Brian Lowans, Craig Lawson. Magic Quadrant for Enterprise Data Loss Prevention. Gartner. 12 September 2023 – ID G00796772.

URL: <https://www.gartner.com/doc/reprints?id=1-2FJYJ0WZ&ct=230912&st=sb>

(дата звернення: 22.10.2025).

6. Market Guide for Data Loss Prevention. Gartner. 2023.

URL: <https://www.gartner.com/en/documents/4018154>

(дата звернення: 22.10.2025).

7. Data Loss Prevention (DLP) Overview. National Institute of Standards and Technology (NIST).

URL: https://csrc.nist.gov/glossary/term/data_loss_prevention

(дата звернення: 22.10.2025).

8. Guide to Data Loss Prevention. SANS Institute.

URL: <https://www.sans.org/white-papers/39055/>

(дата звернення: 22.10.2025).

9. Endpoint DLP – Technical Overview. ManageEngine.

URL: <https://www.manageengine.com/endpoint-dlp/>

(дата звернення: 22.10.2025).

10. ManageEngine Endpoint DLP – Administrator Guide. Zoho Corporation.

URL: <https://www.manageengine.com/endpoint-dlp/help/>

(дата звернення: 22.10.2025).

11. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. International Organization for Standardization.

URL: <https://www.iso.org/standard/82875.html>

(дата звернення: 22.10.2025).

12. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Springer Science+Business Media. 2012.

URL: <https://link.springer.com/article/10.1007/s10796-011-9339-0>

(дата звернення: 22.10.2025).